ATTACHED ATTACHMENTS
SUBMISSION OF COMPUTER FORENSIC SOFTWARE USER MANUALS
CR08-814-PHX-DGC

ATTACHMENT 01	EnCase Forensic v7 Essentials Training OnDemand – v7.04.01i (06.06.2012), **part 1 of 3**; Note: manual broken up into three parts in order to keep attachments under 10mb for PACER.
ATTACHMENT 01	
ATTACHMENT 01	
ATTACHMENT 01

Guidance Software, Inc.
215 N. Marengo Ave., Suite 250
Pasadena, CA 91101

Tel: (626) 229-9191
Fax: (626) 229-9199

e-mail: training@GuidanceSoftware.com
web: www.GuidanceSoftware.com

EnCase® Forensic v7 Essentials

EnCase® Forensic v7 Essentials Training OnDemand – v7.04.01i (06.06.2012)

Guidance Software Training

World-Class Training... Flexible Options

Features & Benefits

- Structured management, budgeting and reduction of training expenses
- Qualify for CPE credits on all classroom courses
- Attendance at all courses, including EnCase® Training OnDemand, qualifies for training hours earned towards EnCE® certification or renewal
- Train in one of our state-of-the-art facilities, at one of our Authorized Training Partners throughout the world, or our EnCE®-certified instructors can come to you
- Customize a course to suit your organization's needs
- Enroll in one of our online courses with EnCase® Training OnDemand
- Enhance professional standing by participating in one or both of our certification programs: the EnCase® Certified Examiner (EnCE®) or EnCase® Certified eDiscovery Practitioner (EnCEP®)

http://www.guidancesoftware.com/computer-forensics-training-certifications.htm

For More Info...

Please contact Guidance Software Training at:
training@guidancesoftware.com
or call 626-229-9191 Ext. 566

Guidance Software Training

The best training available on critical, real-world issues.

Corporations and government agencies use EnCase® software solutions to search, collect, preserve and analyze digital information for the purposes of computer forensics and enterprise investigations, as well as information assurance, e-discovery collection, data loss prevention, compliance with mandated regulations, and more. Guidance Software Training courses and programs help organizations maximize their use of EnCase products.

Guidance Software offers world-class training in enterprise investigations, such as e-discovery and computer security incident response; and in forensic investigations, including all aspects of law enforcement and government examinations.

As the volume and sophistication of digital investigations continue to increase, investigators and examiners can stay ahead of the curve and maintain departmental efficiency by taking advantage of high-level, extensive curriculum, and affordable packages.

Guidance Software has created multiple training options to help ensure your team remains up-to-date and certified on the most current practices in digital investigations.

EnCase® Annual Training Passport

Keep your staff up-to-date with the latest techniques and allow for improved planning.

Organizations must ensure that their investigative staff is properly trained to handle the continually evolving landscape of computer investigations. Budget burdens and scheduling conflicts may limit the amount of training your staff receives. Guidance Software's Annual Training Passport allows you to pay one discounted, flat rate for up to two years of unlimited training for your staff. No other company offers training this extensive at such a deep discount.

EnCase® Annual Passport Fees per student

Program	Price USD	Price GBP
One Year Annual Training Passport	$5,500	£3,437.50
Two Year Annual Training Passport	$10,000	£6,250.00
One Year upgrade	$3,500	£2,187.50
Two Year upgrade	$7,000	£4,375.00

Details, terms and conditions of the program and upgrade options can be viewed at:
http://www.guidancesoftware.com/computer-forensics-training-annual-training-passport.htm

Guidance Training Option Program (GTO)

Take advantage of maximum flexibility in scheduling and course selection.

Organizations must constantly train investigative personnel to maintain the broad-based, changing skill set required for today's digital investigations. With increasing caseloads, personnel changes and unpredictable schedules, meeting this obligation can prove challenging. Guidance Software has developed a solution that addresses these challenges at a practical price. Groups can purchase five or more classes at a reduced rate and use those training seats in the way that best suits your needs.

Program	USD (per seat)	GBP (per seat)
GTO (5-seat minimum)	$2,095	£1,309.38

Fees and restrictions are subject to change. For the most up-to-date information on any of our courses or programs, contact Guidance Software Training at training@guidancesoftware.com or 626-229-9191 ext. 566.

Training Facilities

Los Angeles, CA (Pasadena, CA)
215 North Marengo Avenue
Suite 250
Pasadena, CA 91101

Washington, DC (Dulles, VA)
21000 Atlantic Boulevard
Suite 750
Dulles, VA 20166

Chicago, IL (Rosemont, IL)
9450 West Bryn Mawr Avenue
Suite 200
Rosemont, IL 60018

Houston, TX
1300 Post Oak Boulevard
Suite 550
Houston, TX 77056

London, UK (Slough)
Thames Central, 5th Floor
Hatfield Road, Slough, Berkshire
UK SL1 1QE

We also have Authorized Training Partners all over the world

For a complete listing visit:

http://www.guidancesoftware.com/computer-forensics-training-partners.html

EnCase® Mobile Training Courses

If your organization needs EnCase® training, but does not have a computer training laboratory or a travel budget, this program is designed for you. Guidance Software brings all the necessary equipment and materials to your site and our instructor conducts the course. This program is ideal for organizations with limited travel budgets, as well as those who need to train a number of employees at the same time, but cannot afford to have so many of their personnel away. Students receive the same high-quality instruction as they would at a Guidance Software training facility.

The pricing is the same as our regular instructor-led courses with the following additional charges:

Program	Price USD	Price GBP
Training Instructor Fee - 1 instructor / up to 12 students	$4,500	£2,812.50
Training Instructor Fee - 2 instructors / 13 to 24 students	$9,000	£5,625.00
Standard Shipping U.S.	$500	
Standard Shipping International	$800	£500.00

For a complete list of mobile options call Guidance Software Training at 626-229-9191 ext. 566 or visit our website at:

http://www.guidancesoftware.com/computer-forensics-training-mobile-onsite.htm

EnCase® Certified Computer Examiner (EnCE®) Certification Bootcamp

The EnCE® certification has become the gold standard for digital examiners. With this program, students can prepare for certification while learning how to maximize their use of EnCase® software and solutions. The bundle provides all required training and test preparation for EnCE® certification. Students participating in this bootcamp take advantage of three courses: the EnCase® OnDemand Computer Forensics I, EnCase® OnDemand Computer Forensics II, and the EnCase® EnCE® Prep course, which is taken in the classroom. On the final afternoon of the EnCE® Prep course, the EnCE® written examination will be administered to the students in a monitored, timed environment.

	Price USD	Price GBP
EnCE® Certification Bootcamp	$4,485	£2,803.13

Fees and restrictions are subject to change. For the most up-to-date information on any of our courses or programs, contact Guidance Software Training at training@guidancesoftware.com or 626-229-9191 ext. 566.

Our Customers

Guidance Software's customers are corporations and government agencies in a wide variety of industries, such as financial and insurance, technology, defense, energy, pharmaceutical, manufacturing and retail. Our EnCase® customer base includes more than 100 of the Fortune 500 and more than half of the Fortune 50, including: Allstate, Chevron, Ford, General Electric, Honeywell, Northrop Grumman, Pfizer, UnitedHealth Group and Viacom.

About Guidance Software (NASDAQ: GUID)

Guidance Software is recognized worldwide as the industry leader in digital investigative solutions. Its EnCase® platform provides the foundation for government, corporate and law enforcement organizations to conduct thorough, network-enabled, and court-validated computer investigations of any kind, such as responding to eDiscovery requests, conducting internal investigations, responding to regulatory inquiries or performing data and compliance auditing - all while maintaining the integrity of the data. There are more than 40,000 licensed users of the EnCase technology worldwide, the EnCase® Enterprise platform is used by more than sixty percent of the Fortune 100, and thousands attend Guidance Software's renowned training programs annually. Validated by numerous courts, corporate legal departments, government agencies and law enforcement organizations worldwide, EnCase has been honored with industry awards and recognition from *Law Technology News*, *KMWorld*, *Government Security News*, and *Law Enforcement Technology*.

ENCASE® FORENSIC V7 ESSENTIALS TRAINING ONDEMAND
CONTENTS

Getting Started with EnCase

ENCASE® FORENSIC V7

EnCase Forensic v7 (EnCase v7) is the next advancement in computer forensics technology, workflow, and best practices.

With powerful automation capabilities, streamlined user interface, and optimized case management, EnCase v7 will transform how you perform investigations. Just a few of the paradigm-shifting features are:

- Intuitive, streamlined interface
- Powerful processing capabilities
- Find evidence faster with unified search
- Review e-mail the way you want it
- Smartphone acquisition
- Quick case access
- Increased scalability

At the core of EnCase v7 is our commitment to robust file and operating system support. With version 7, you will be able to investigate more file and operating systems than ever before.

Leveraging the indexing engine from our EnCase® Command Center (EnCase® eDiscovery and EnCase® Cybersecurity) products, you will now have search results across multiple types of files all in one location, including files, e-mail, instant message (IM) conversations, Smartphones, etc.

- Dramatically change the workflow through the product to improve efficiency through automation
- Harness the power of indexing and searching versus browsing for the "needle" of evidence in the ever-increasing volume of the digital "haystack"
- Use the index to build relationships between items throughout EnCase v7, including items from EnScript® processing and Smartphone acquisitions
- Increase the usability of the software to find evidence faster

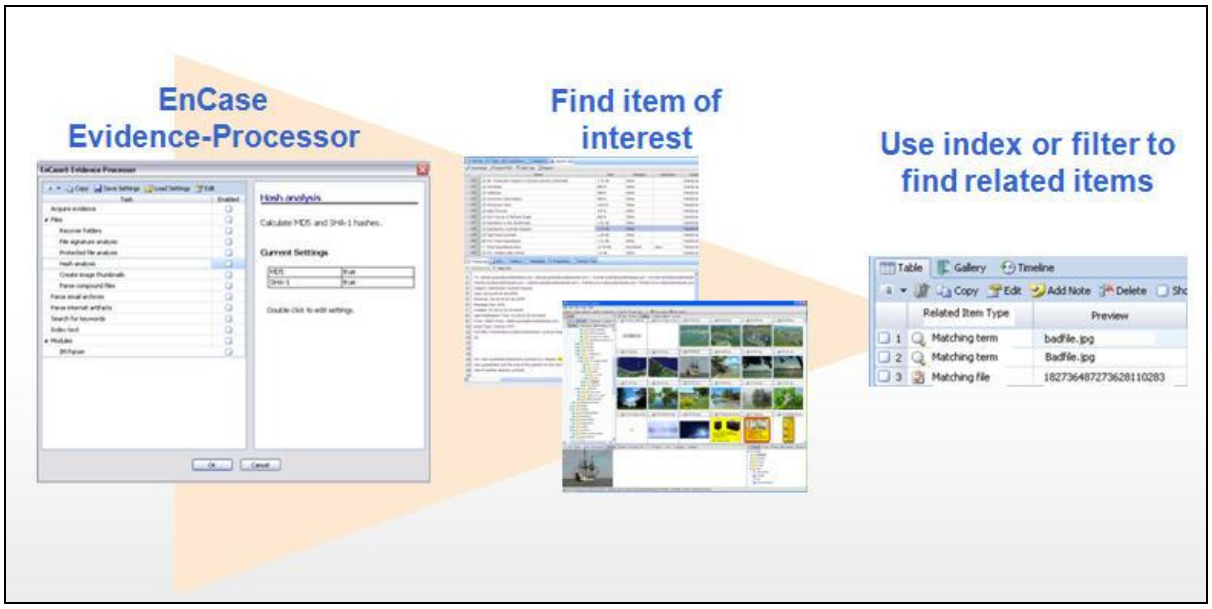

Figure 1-1 New workflow in EnCase v7

NOW INCLUDED STANDARD IN ENCASE V7

The EnCase Forensic modules are now all included in v7, including:

- Smartphone support
- EnCase® Decryption Suite (EDS) – Provides the ability to decrypt supported full disk and volume encryption and encrypted registry entries
- EnCase® Physical Disk Emulator (PDE) Module – Mount evidence files, including deleted files, as a virtual physical disk on your computer
- EnCase® Virtual File System (VFS) Module – Mount evidence files as an offline network share in your Windows® operating system
- EnCase® FastBloc Software Edition (SE) – Software write blocker ensures that no writes occur to a removable device during preview or acquisition

Encryption Support

EnCase v7 supports the following encryption products.

Vendor	Product	Supported Versions	64-bit Support
Check Point	Check Point Full Disk Encryption (formerly Pointsec PC)	6.3.1 up to 7.4	Yes
CREDANT	Mobile Guardian	5.2.1, 5.3, 5.4.1, 5.4.2, 6.1 through 6.8	No
GuardianEdge	Encryption Plus/Anywhere	7 and 8	No
GuardianEdge	Hard Disk Encryption	9.2.2 , 9.3.0, 9.4.0, 9.5.0, 9.5.1	Yes
McAfee	SafeBoot	4.5, 6 (Windows and Macintosh)	No
Microsoft	BitLocker and BitLocker To Go	Vista, 7	Yes
Sophos	SafeGuard Easy (formerly Utimaco)	4.5, 5.5	Yes
Symantec	PGP Whole Disk Encryption	9.8, 9.9, 10	Yes
Symantec	Endpoint Encryption	7.0.2, 7.0.3, 7.0.4, 7.0.5, 7.0.6, 7.0.7, 7.0.8, 8.0	Yes
WinMagic	SecureDoc Full Disk Encryption	4.5, 4.6	No

Major Improvements In EnCase v7

In addition to the enhanced workflow, you will notice a number of improvements in the functionality of EnCase v7:

- No longer will you have to wait for a case to open. File system, e-mail, and other compound structures will now have their structures cached out to disk, so you are no longer restricted in the amount of memory you have on disk when viewing large amounts of data.
  - EnCase v7 will be able to bring these items into memory as needed when navigating through the case.
- You can now mark files with user-defined tags to help remember important information about the file. These tags can be used later for filtering and reporting.
- We have streamlined the number of configuration items; for example the view for configuring file types, file signature, and file viewers have been combined into File Types.

- We have made the configuration settings accessible at the time that you are accessing that area; for example Text Styles are now set in the text pane itself.
- We've separated EnCase v7 configuration settings from user settings. This allows us to update the delivered configuration files while leaving your files untouched.
- The Evidence Processor helps automate your work in preparing for an investigation.
- Viewing and working with e-mail is easier in EnCase v7.
- Searching is more powerful and has a new index engine.
- There are new templates for customize reports.
- Smartphone support is included.
- New file system and file type support:
  - EXT4, including Linux Software RAID 1 and 10 Arrays for Ubuntu version 9.1 and version 10.04
  - HFSX
  - Microsoft® Office 2010 support
  - Check Point®/Pointsec™

INSTALLING ENCASE FORENSIC V7

To install EnCase v7:

1. Obtain the most current installation file available or insert the EnCase® Forensic installation DVD into your drive
   - If the installation does not auto start from the DVD, browse to locate and run Setup.exe

2. The welcome page of the install wizard appears
   - Note that the bottom right corner of the dialog displays the version of EnCase that will be installed into this path first, followed automatically by EnCase v7

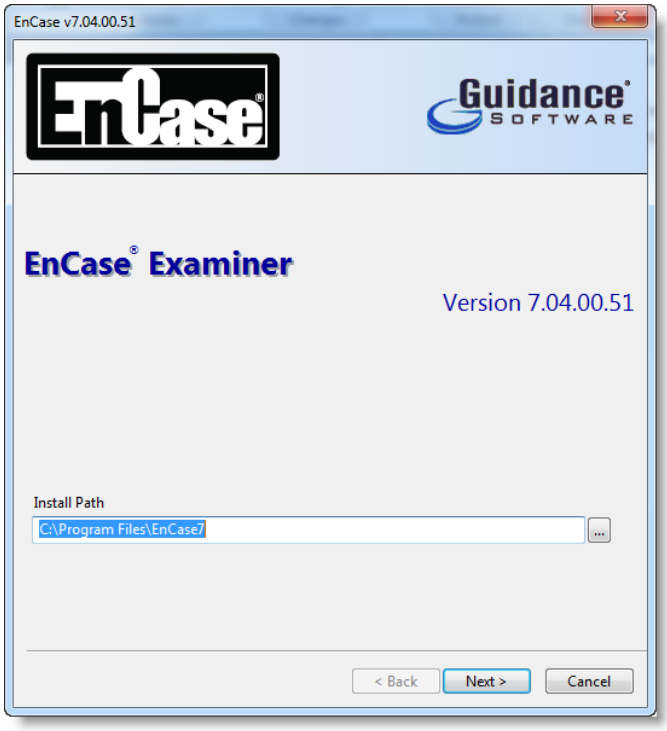

Figure 1-2 Welcome screen of installation wizard

3. Click **Next>**
4. If the folder does not yet exist, click **Yes**

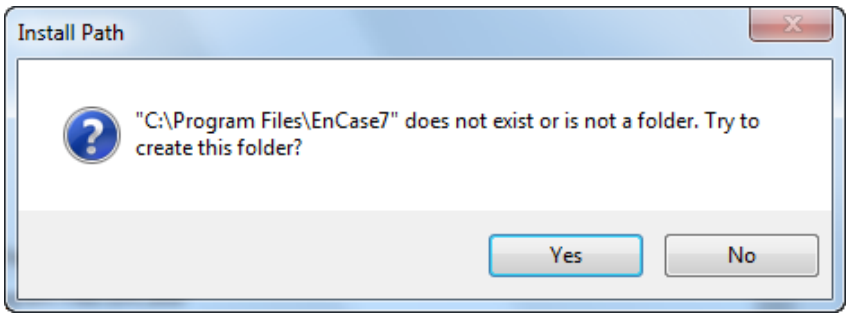

Figure 1-3 Click "Yes" to create a new folder

5. If you are upgrading, click **OK** or **Cancel** to go back and change the installation folder.

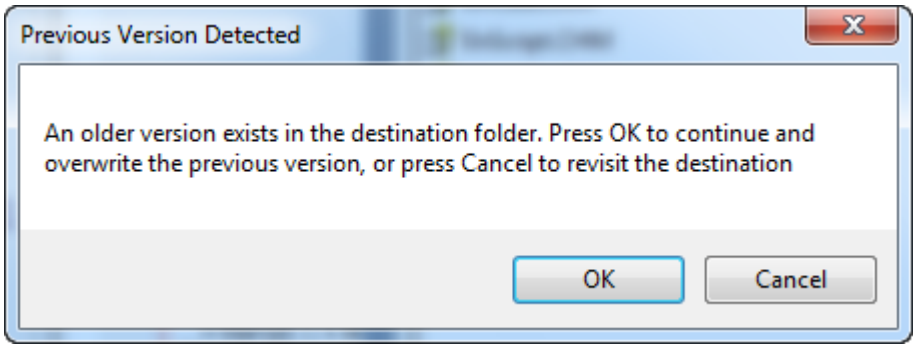

Figure 1-4 Select option to change installation folder

6. Following is a license agreement page for EnCase Forensic
7. Read and acknowledge your acceptance of the license agreement by clicking **Next>**

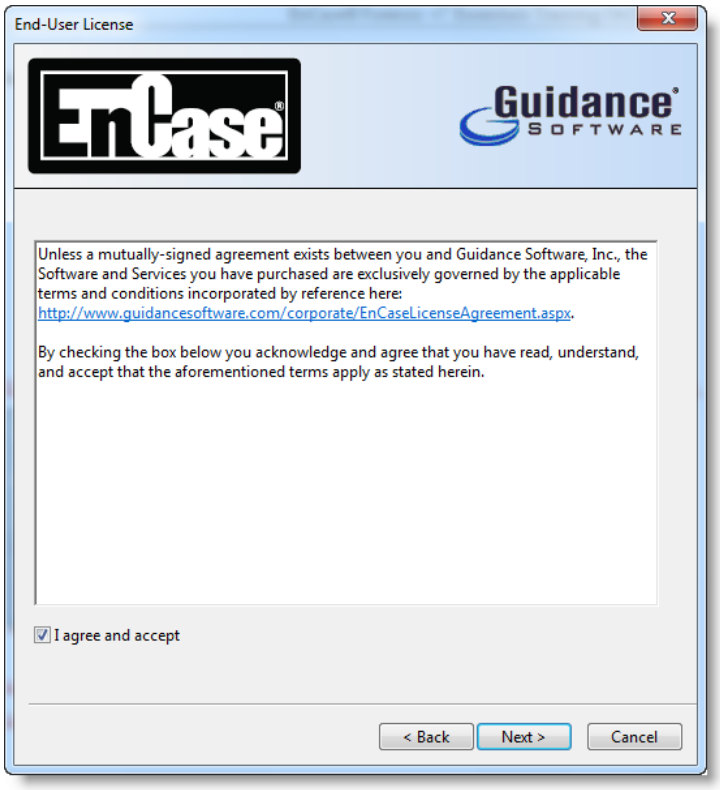

Figure 1-5 License Agreement

8. The next window offers to install additional properties if it is a first-time installation with no security key drivers installed

   NOTE: If this is the first installation of EnCase® software, remove any dongles and check the box next to **Install HASP Drivers** to install or upgrade the drivers needed for the EnCase® dongles.

9. Click **Next>**

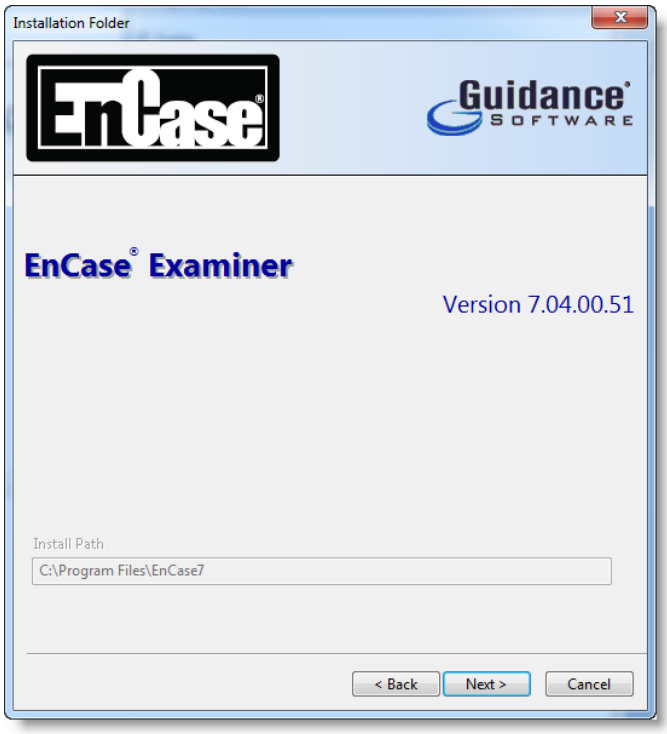

Figure 1-6 Installation path

- You should see that the setup has completed successfully

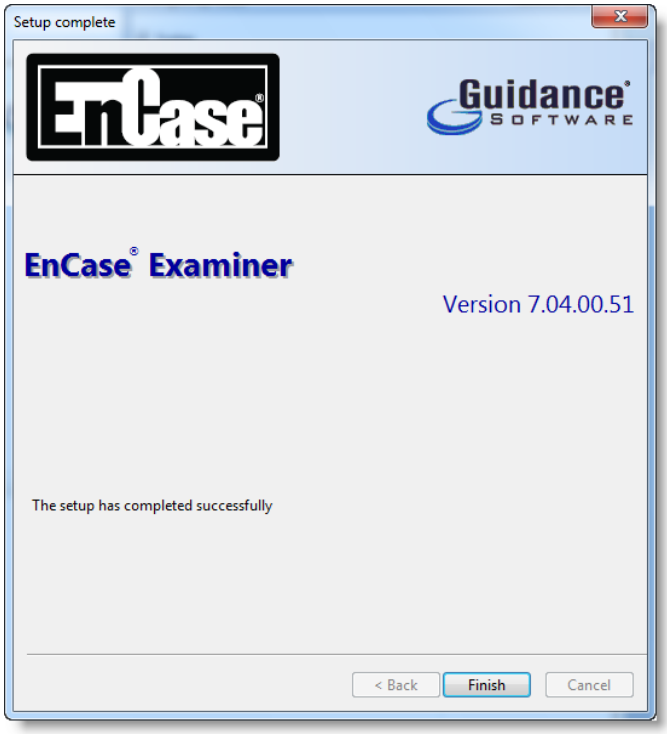

Figure 1-7 Successful installation

10. You may be notified that your system should be rebooted; to ensure the registration of certain DLLs and enable the drivers, etc., it is strongly encouraged to reboot at this time
11. Make the reboot selection and click **Finish**

With the program successfully installed, the shortcut to EnCase v7 will appear on your Desktop.

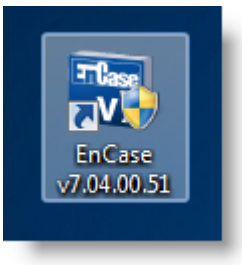

Figure 1-8 Program icon

INSTALLING THE CERT FILE

The next step is to install the cert files. If you have cert files to install, those files need to be copied into the Certs folder. By default the location is:

```
C:\Program Files\EnCase7\Certs
```

NOTE: With Windows 7 and Vista, you will need to copy the cert files onto your hard drive from the Internet and then copy them into the `C:\Program Files\EnCase7\Certs` directory. The security permissions of Windows 7 and Vista prevent direct copying from e-mail or the Internet into `C:\Program Files`.

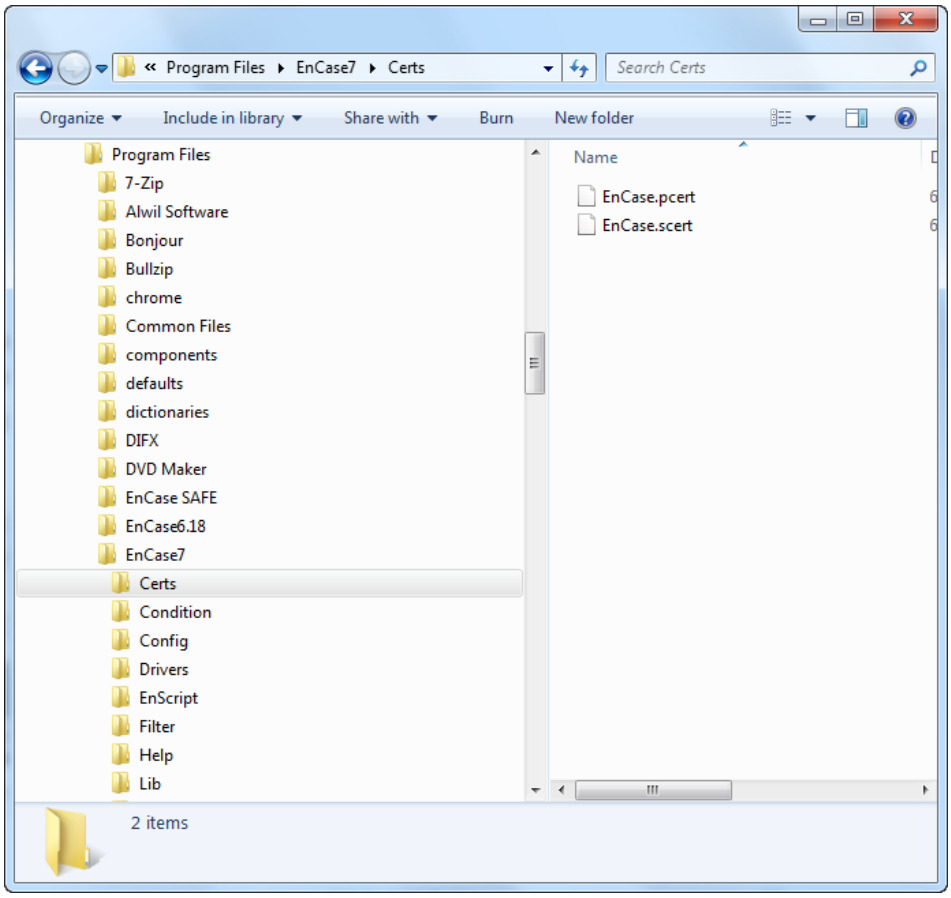

Figure 1-9 Install cert files into the Certs folder

RUNNING ENCASE

Double-click on the EnCase v7 icon on your Desktop to run EnCase for the first time.

Please take a moment to register you EnCase v7.

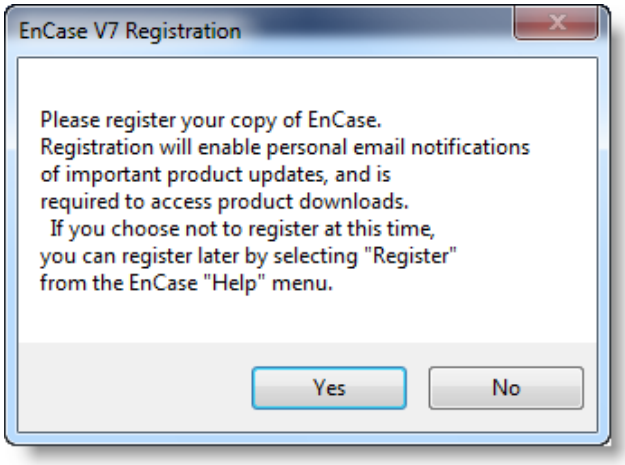

Figure 1-10 Register EnCase Forensic v7

Follow the instructions on the webpage, depending if you have Internet connectivity

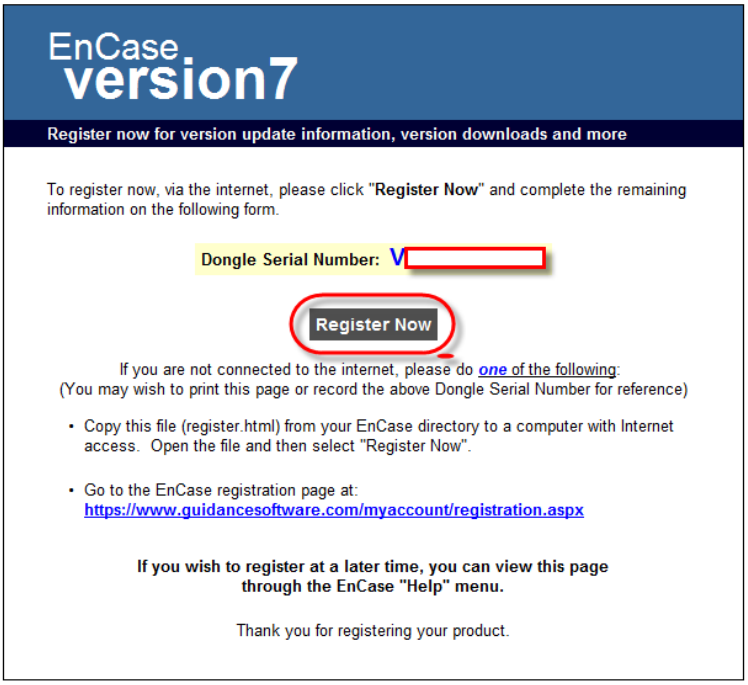

Figure 1-11 Register EnCase Forensic v7

EnCase will open to the Home screen.

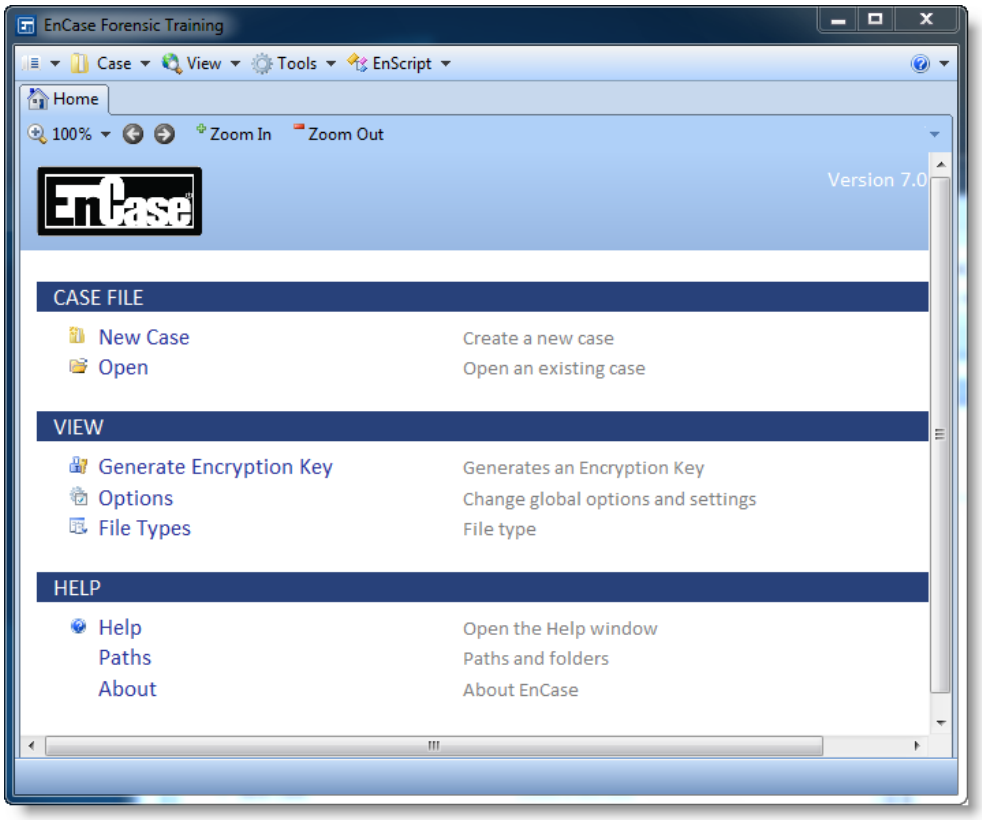

Figure 1-12 EnCase Forensic v7

Notes

Notes

Notes

EnCase® Concepts

EnCase® Forensic

EnCase Forensic v7 (EnCase v7) provides investigators with a single tool for conducting large-scale and complex investigations from beginning to end. It features superior analytics, enhanced e-mail/Internet support, and a powerful scripting engine.

With EnCase v7 you can:

- Acquire data in a forensically sound manner using software with an unparalleled record in courts worldwide
- Investigate and analyze data from multiple platforms – Windows, Linux, AIX, OS X, Solaris, and more – using a single tool
- Find information despite efforts to hide, cloak, or delete
- Easily manage large volumes of computer evidence, viewing all relevant files, including deleted files, file slack, and unallocated space
- Transfer evidence files directly to law enforcement or legal representatives as necessary
- Review options that allow non-investigators, such as attorneys, to review evidence with ease
- Use reporting options for quick report preparation

Forensically Sound Acquisitions

EnCase v7 produces an exact binary duplicate of the original drive or media, then verifies it by generating MD5 and/or SHA1 hash values for related image files and assigning Cyclic Redundancy Check (CRC) values to the data (when no compression is used). These checks and balances reveal any inconsistencies with acquired data. EnCase v7 maintains the reliability and functionality of previous versions while simplifying usage, adding powerful new features, and significantly increasing performance.

EnCase v7 is accessible to several types of users:

- Those responsible for collecting evidence
- Forensic examiners and analysts
- Forensic examiners who develop and use EnScript® code to automate repetitive or complex tasks

Forensic Workflow

EnCase v7 facilitates the forensic workflow process through the:

1. Preview and processing of case data
2. Analysis of evidence
3. Reporting of findings

EnCase® Evidence .Ex01 and .Lx01 v2

EnCase v7 has new evidence file (.Ex01) and logical evidence file (.Lx01) formats..

The existing EnCase® evidence file has performed well for over a decade. It is court-validated, well-known, and adopted in the industry. Despite its effectiveness, some limitations remain that can only be overcome with an updated evidence file format.

Many of the central design principles of the E01 format have been retained. The Ex01 format still stores data in blocks that are verified with an individual 32-bit CRC (when no compression is used), and all of the source data stored in the file is hashed with the MD5 and/or SHA1 algorithms if requested by the user.

The Ex01 enhancements do not affect features of the file, such as those that have been relied upon by many courts to rule on the acceptance of the file as a container of original evidence; the additions merely facilitate the ability to track and handle new characteristics of the stored data.

The new Ex01 format introduces the following capabilities:

- Support for encryption of the data
- Ability to use different compression algorithms
- Improved support for multi-threaded acquisitions where sectors can be out of order
- Efficient storage and handling of sector blocks that are filled with the same pattern (such as 00-byte fills)
- Alignment considerations to improve efficiency and performance
- Improved support for resuming acquisitions
- Internal improvements of the data structures

E01 had the ability of using a "soft" password, meaning that the data itself was not encrypted. Ex01 encrypts the data symmetrically, using AES-256 by default. The encryption key for this can be protected with:

- A password that generates a symmetric key
- An asymmetric key pair
- Both of the above

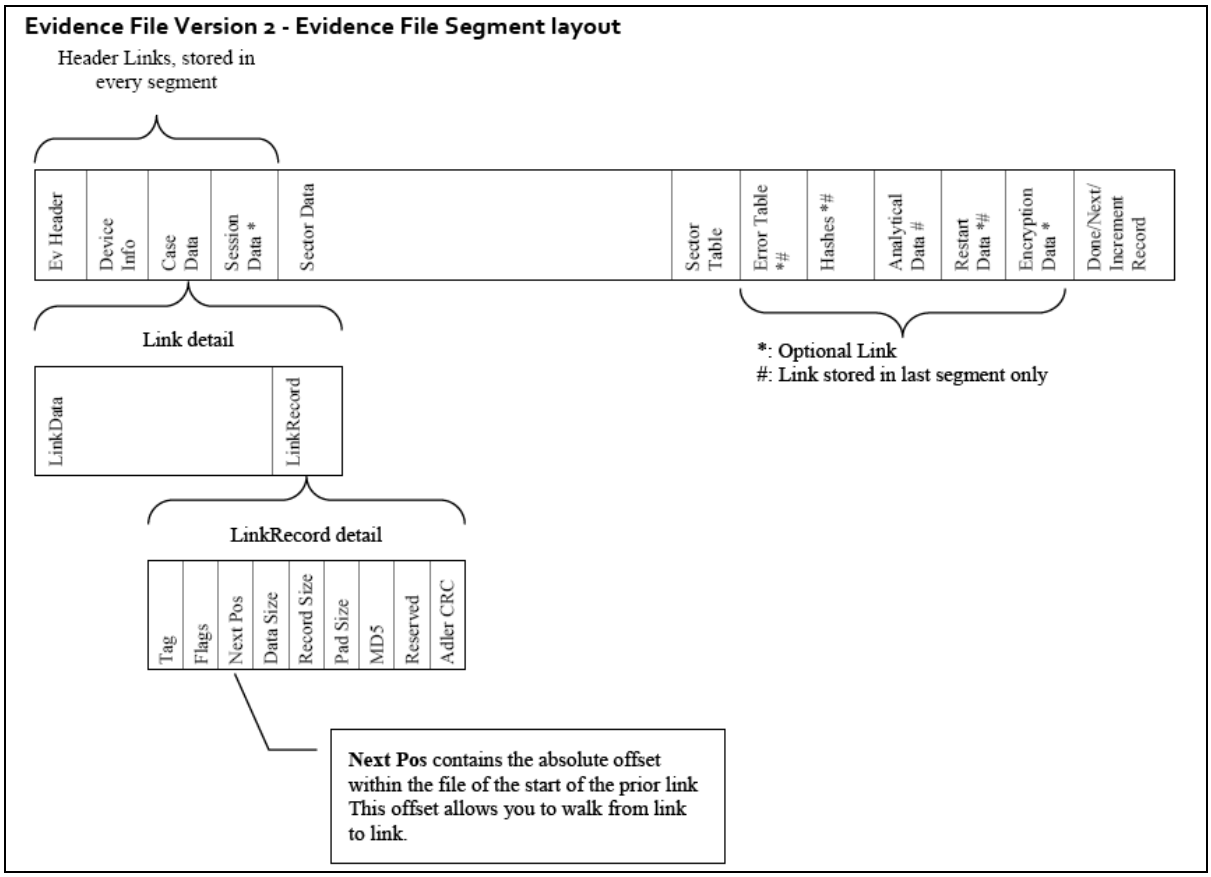

Figure 2-1 New EnCase® evidence file format

For instruction on acquiring digital evidence, please consider one or more of the following courses:

Course	Course website
First Responder with EnCase® Forensic, Tableau, and EnCase® Portable	http://www.guidancesoftware.com/EnCase-First-Responder.htm
EnCase® Computer Forensics I	http://www.guidancesoftware.com/computer-forensics-training-encase1.htm
EnCase® Portable Configuration and Examinations	http://www.guidancesoftware.com/encase-portable-examinations.htm

CASE FILE

In prior versions of EnCase, the case file is a text file that contains information specific to one case. In EnCase v7, a case is no longer contained within a single file, but is stored within a folder containing many components. The case contains pointers to any number of evidence files or previewed devices, bookmarks, search results, sorts, hash analysis results, signature analysis reports, etc. Before media can be previewed or evidence files analyzed, a case file must be created when you run EnCase. The case cannot be simultaneously accessed by more than one examiner at a time. In EnCase v7, the default location for saving the case files is the User Data folder.

Verifying an Evidence File Automatically

Whenever an evidence file is added to a case, EnCase v7 will begin to verify the integrity of the entire disk image in the background. This is usually quite fast for small (removable devices) evidence files, but can take longer for hard disk evidence files. You may begin the examination while the verification occurs.

ENCASE® CONFIGURATION FILES

Prior to EnCase v7

In prior versions of EnCase, configuration files were contained in a series of initialization (.INI) files that contained global settings for EnCase. These files contained the signature table, file types, file viewers, filters, global keywords, etc. These files applied global configurations to every case and evidence file used within the EnCase® environment. They were stored (by default) in the folder where EnCase is installed, usually `C:\Program Files\EnCase6\Config`.

Configuration Changes in EnCase v7

In EnCase v7, there are major changes in the way EnCase stores configuration settings. These changes were necessary to better support the Windows operating systems (specifically Vista and Windows 7) protocols in regards to user and application data management. Windows guidelines encourage all user data to be stored in specific locations to facilitate better system security and a better customer experience (customers can go to one place to find their data). Likewise, Windows encourages applications to put volatile data in an Application data area, so that it is clear to you what data is part of an application and what data is considered user data.

An additional benefit of these changes in v7 is the resolution of a long-standing issue with updating .ini files. In prior versions, if you modified your FileTypes.ini file, you would not receive updates to those files from Guidance Software as they would write over your custom configuration.

Configuration Files Locations

The following location list defines the areas used by EnCase v7 and gives a brief description of which types of files should reside in which location:

- **User Data**
  (`C:\Users\<username>\My Documents \EnCase`)
  - This folder is for user-created files that are not necessarily EnCase-version or installation specific. Files like case files and EnScript® files would default to this folder.
- **User Application Data**
  (`C:\Users\<username>\AppData\Roaming\EnCase1`)
  - This folder is for configuration files and user temp files that pertain to a specific user and installation folder of EnCase (Window sizes, fonts, etc.)
- **Global Application Data**
  (`C:\Users\Default\AppData\Roaming\<EnCase-1>`)
  - This folder contains files that are for the configuration of EnCase regardless of the user (NAS settings, etc.)
- **Program Files Folder**
  - This folder contains files that are created by the installer and are unmodified by the application
- **Shared Files Folder**
  - This folder can be pointed to a folder where you keep shared files (EnScript® modules, Searches, Conditions, File Types, Text Styles, and Keys)

EnScript® Programs

EnScript programs are saved in two or three directories:

- The EnScript modules shipped with EnCase continue to be stored in the `C:\Program Files\EnCase7\EnScript` folder
- Your EnScript programs are now stored in your user folder under `C:\Users\<userfolder>\EnCase\EnScript`
- You can also specify a shared folder to be able to browse to your EnScript® library

You now run your EnScript modules from the toolbar drop-down instead of the former tree control in the lower right pane.

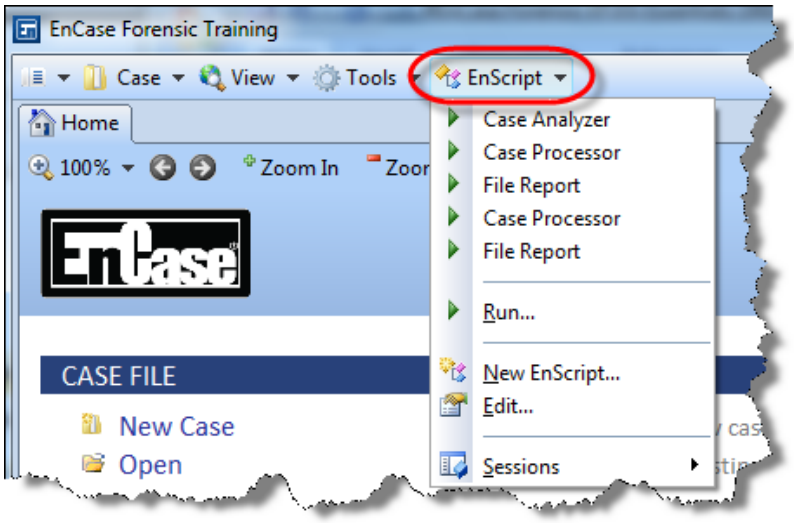

Figure 2-2 EnScript toolbar

When you select **Run...** or **Edit...**, you are presented with a file selection dialog that allows for easy browsing to all of the default locations via an EnCase tree on the left side.

NOTE: On operating systems prior to Windows Vista, this functionality will not be available and you will need to manually navigate to the EnCase v7-shipped EnScript folder or your shared folders.

Filters and Conditions

Filters and conditions were previously all saved in a single .ini file in the `C:\Program Files\EnCase6\Config` directory. In EnCase v7, filters and conditions are now being saved in individually named files with the extension `.EnFilter` or `.EnCondition`, respectively.

The filters you create are saved in a separate folder from the EnCase delivered filters. This allows you to create and edit you own filters and removes the need for overwriting similarly named filters or the wholesale loss of your filters when there is an EnCase update.

The functions for selecting and creating filters are the same as EnScript modules.

File Viewers

There are no default viewers shipped with EnCase v7, so any viewers you add will be saved in an .ini file that only exists in your user directory.

Text Styles

Text styles are split into separate files and are viewable by you in a settings dialog that separates your user entries from the Guidance Software delivered entries with tabs.

File Types Combined with Signatures

File Types and File Signatures are combined into a single table. These are handled as two or three separate settings files; your user settings will override the shipped and shared settings.

In this case a new column is displayed that shows you the items that have been modified by you. When you change an item or create new items, these items are identifiable by the User Modified column.

If you want to get back the default settings for an item, select the item and then choose **Reset to Default** to get the Guidance Software default settings for the item.

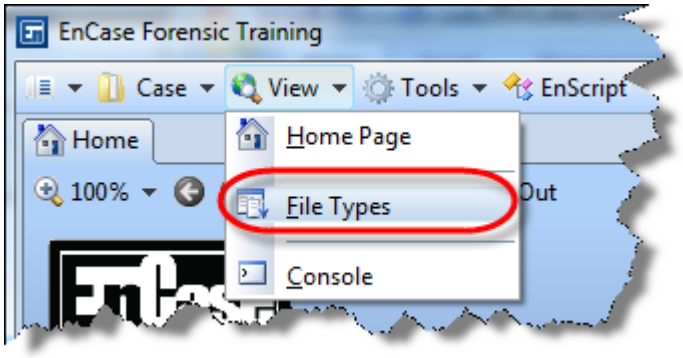

Figure 2-3 File Types View

ENCASE V7 APPLICATION FOLDER LOCATIONS

Application Folder

This folder contains files created by the EnCase installer that are ***not*** modified by EnCase.

- Windows 7 and Windows Vista default path: `\Program Files\EnCase7`
- Windows XP: `\Program Files\EnCase7`

Folder Name	Description
Certs	License certificates
Condition	Default conditions
Config	Application configuration options
Drivers	Application drivers
EnScript	Default EnScript programs
Filter	Default filters
Help	Help files
Lib	Application library files
License	EnLicense files
Mobile	Mobile phone drivers
Noise	Default noise file for the Index
Template	Default case templates
ViewLib	Outside in libraries

User Data

The following are user-created files that are not necessarily EnCase-version or installation specific:

- Windows 7 and Windows Vista path: `\Users\<Username>\My Documents\EnCase`
- Windows XP: `\Documents and Settings\<Username>\My Documents\EnCase`

Backup:

- Windows 7 and Windows Vista path: `\Users\<Username>\My Documents\EnCase`
- Windows XP: `\Documents and Settings\<Username>\My Documents\EnCase`

Folder Name	Description
Condition	User-defined conditions
EnScript	User-defined EnScript modules
Filter	User-defined filters
Keys	Encryption keys
Keyword	User-defined keyword searches
Logs	Console logs
Search	User-defined searches
Template	User-defined case templates

Case Folder

This folder contains all files that make up an EnCase v 7 case:

- Windows 7 and Windows Vista default path: `\Users\<Username>\My Documents\EnCase\<Case Name>`
- Windows XP: `\Documents and Settings\<Username>\My Documents\EnCase\<Case Name>`

Item	Description
Corrupt Pictures	Corrupt pictures
E-mail	E-mail thread database
Export	Default case export folder
Results	Results of search queries
Searches	Keyword search results (non-Evidence Processor)
Tags	Tag database
Temp	Default case temp folder
<Case Name>.Case	EnCase case file

Evidence Cache

This folder contains the cache, index, and keywords results for a device that are created by the EnCase® Evidence Processor:

- Windows 7 and Windows Vista default path: `\Users\<Username>\My Documents\EnCase\Evidence Cache\<Hash>`
- Windows XP: `\Documents and Settings\<Username>\My Documents\EnCase\Evidence Cache\<Hash>`

Item	Description
Device Cache	Device caches
DeviceIndex	Device index
Searches	Keyword search results (Evidence Processor)

User Application Data

This folder contains configuration files and temporary user files associated with a specific user and EnCase installation folder.

- Windows 7 and Windows Vista path: `\Users\<Username>\App Data\Roaming\EnCase\EnCase7-<#>`
- Windows XP: `\Documents and Settings\<Username>\Application Data\EnCase\EnCase7-<#>`

Folder	Description
Config	User-edited application configuration files

Global Application Data

This folder contains files that are used to configure EnCase v7 regardless of the user:

- Windows 7 and Windows Vista path:
  - `\ProgramData\EnCase\EnCase7-<#>`
- Windows XP:
  - `\Documents and Settings\All Users\Application Data\EnCase`
  - `\Documents and Settings\All Users\Application Data\EnCase\EnCase7-<#>`

NOTE: `\Users\All Users\AppData = \ProgramData`

Item	Description
Logos	Default report logo
Config	NAS and other global configuration files
ParseCache	Parse cache files
Storage	EnScript configuration files

Shared Files

This is a folder location in which you store shared files, such as EnScript programs, searches, conditions, keys, file types, text styles, and so forth.

- Windows 7 and Windows Vista path: `<User Defined>`
- Windows XP: `<User Defined>`

ENCASE V7 GRAPHICAL USER INTERFACE

The significant changes to the Graphical User Interface (GUI) are detailed as follows.

Web Browser-like Tabs

The new tabs are used as destinations for information, such as browsing file entries, searching the index, and configuration. You can choose the tabs that you would like to have visible, and you can have multiple instances of certain types of tabs open, which allows the browsing and searching of multiple items.

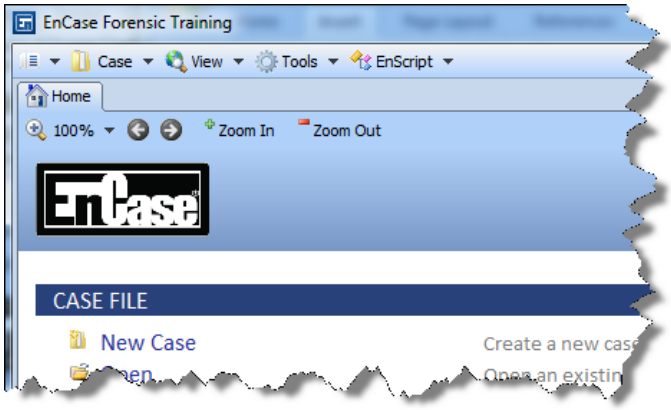

Figure 2-4 Browser-like tabs

What's New in EnCase v7 versus v6

There are several changes to the GUI for EnCase v7 that improve the workflow and efficiency of computer forensic examinations.

- **Bottom Right Pane Removed** – There is no longer a general-purpose, bottom right-hand pane. This gives you more control over what you are viewing and dramatically reduces the number of tabs you need to navigate.
- **Main Application Tool Bar Removed** – The old text menu bar with applications was removed. There are now top-level, drop-down menus that provide greater flexibility.

Figure 2-5 Top-level, drop-down menus

- **New Side Bar Menu** – Each pane now has a side bar menu for common functions, such as Conditions, Filters, and Tags.

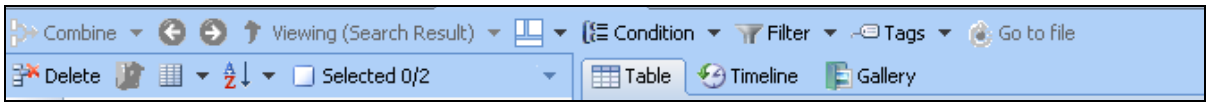

Figure 2-6 Side bar menus

- **Flexible Pane Layouts** – Rather than the static four panes of v6, you can set a preferred layout for each view:
  - Table
  - Tree-Table
  - Traeble
  - Tree

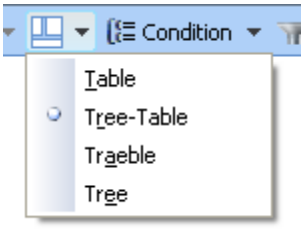

Figure 2-7 Flexible pane layouts

- **Floating Box for Text** – If the data in a table cell is truncated by the column size, hovering over it will display the content in a floating box.

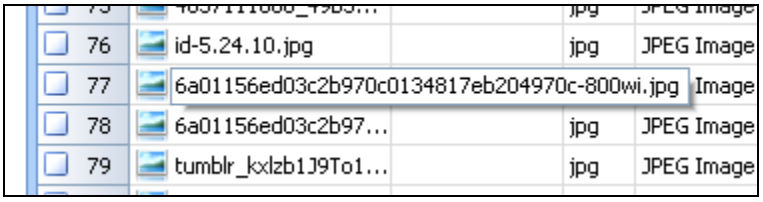

Figure 2-8 Floating text box

- **Tabs for Multi-dimensional Cell Data** – The bottom pane contains tabs for multi-dimensional data, such as Fields, Permissions, Hash Set Properties, and File Extents. This is different from the single Additional Details tab in v6, and the tabs are available regardless of what cell is currently highlighted.

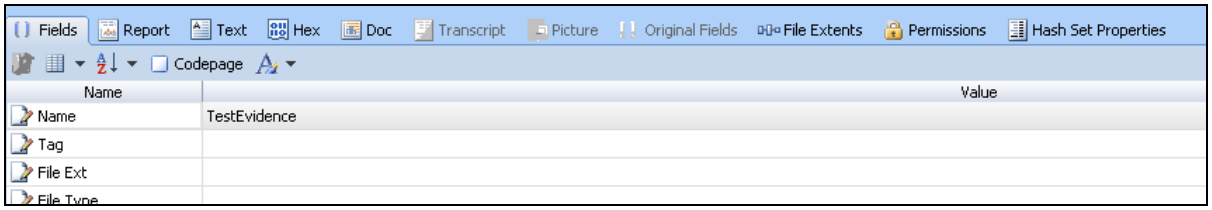

Figure 2-9 Multi-dimensional cell data tabs

- **Drop-down Menus** – In contrast to the trees in v6, you now have drop-down menus for selecting functions; for example:
  - **Text Styles** – Now available via a drop-down menu in the **Text→Hex→Transcript** view
  - **Filters** – Now available via a drop-down in the View Pane top menu bar.

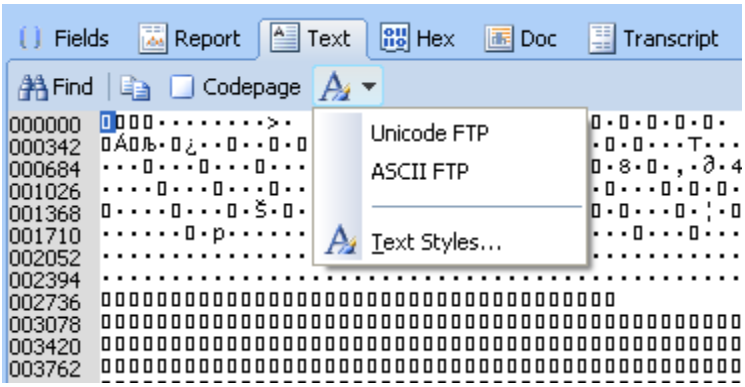

Figure 2-10 Drop-down menus

- **Configuration Settings** – The configuration items are now accessible where they are needed. For example, you can create and/or select keywords at the time the search is executed, such as under **Raw Search All...**

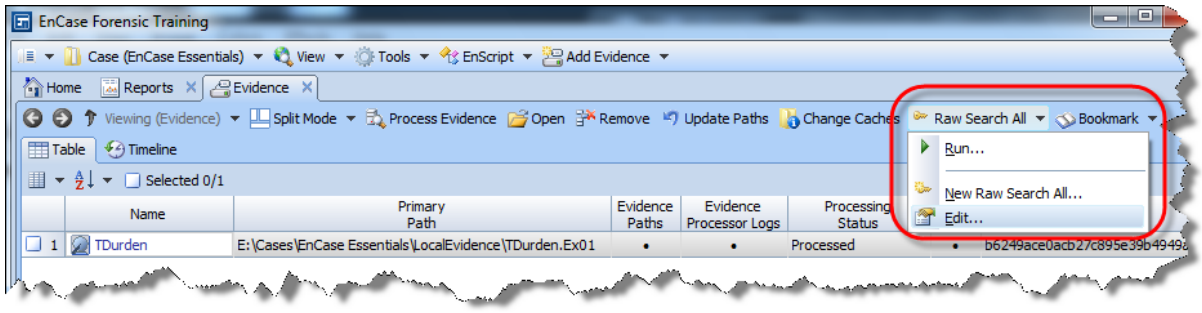

Figure 2-11 Configuration

VIEW MENUS

The following is a summary of the major changes in the EnCase v7 GUI.

EnCase v6 Function	EnCase v7 Location
Archive Files	Removed
Cases	Cases drop-down menu
Encryption Keys	Accessed where used
File Signatures	Removed (merged with File Types)
File Types	Accessed where used; View drop-down menu
File Viewers	Accessed where used
Hash Sets	Accessed where used; View drop-down menu
Keywords	Accessed where used; Entries Keyword Search toolbar item
EnScript	To EnScript drop-down
Filters	To Filter drop-down on Entries, Records, Search Results
Conditions	To Condition drop-down on Entries, Records, Search Results
Display	To individual Filter tabs
Queries	No longer a function in EnCase
Text Styles	To drop-down above Text/Hex/etc., view

Notes

Notes

Notes

How to Create a Case

One of the most powerful features of EnCase® v7 is its ability to organize different types of media together, so that they can be indexed and searched as a unit rather than individually. This process saves time and allows you to concentrate on examining the evidence.

Case Management

Before starting an investigation and acquiring media, consider how the case will be accessed once it has been created. It may be necessary for more than one investigator to view the information simultaneously. In such an instance the evidence files should be placed on a central file server and copies of the case file should be placed on each investigator's computer (since case files cannot be accessed by more than one person at a time).

The EnCase® Forensic methodology strongly recommends that you use a second hard drive, or at least a second partition on the boot hard drive, for the acquisition and examination of digital evidence. It is preferable to wipe an entire hard drive or partition rather than individual folders to ensure that all of the temporary, suspect-related data is destroyed. This will aid in deflecting any claims of cross contamination by the opposing counsel if the forensic hard drive is used in other cases. Of course the evidence in the EnCase® evidence files is always protected from cross-contamination.

One method of organization is to create a folder for each case and to place the associated case file and evidence files in that folder. Reports and evidence copies can then be placed in the same folder or in subfolders.

Create a Cases folder on your evidence drive for case management.

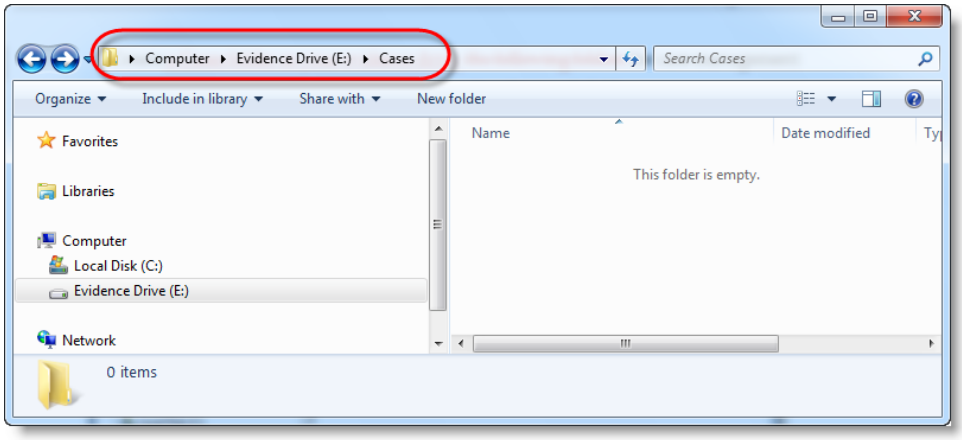

Figure 3-1 Creating the folder structure

Start EnCase v7.

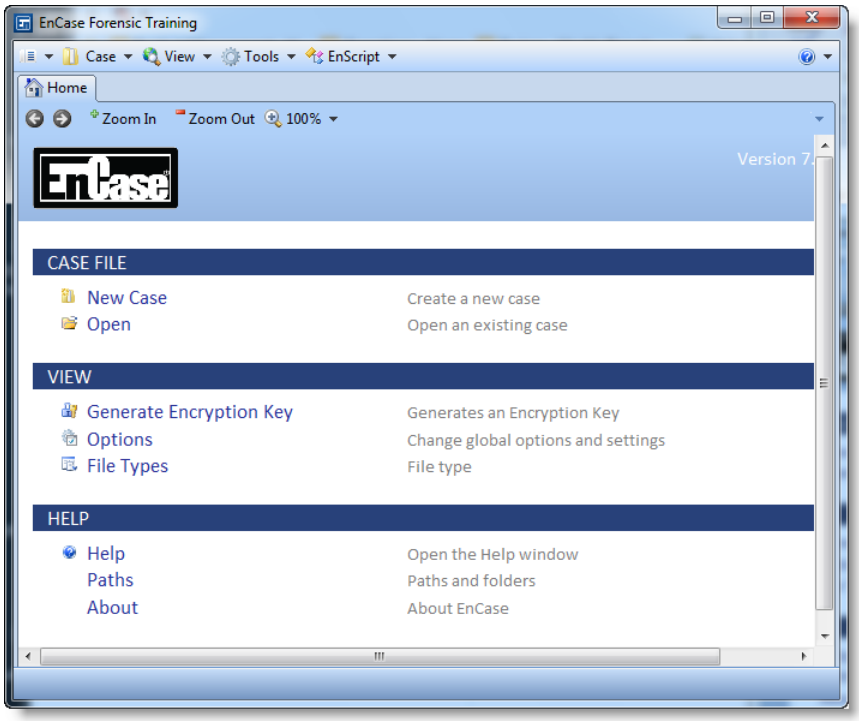

Figure 3-2 EnCase v7

The **Home** page, like all pages within EnCase, is divided into several sections, each with a specific set of functions. In descending order, they are as follows:

Application Toolbar	Appears below the title bar and provides drop-down menus to major functionality. The menus and their selections are primarily static throughout your investigation. The menus and their selections are discussed in more detail later in this lesson.
Tabs	Similar to tabs in Internet browsers, each top-level tab displays a page that groups EnCase functionality. When you open EnCase for the first time, only the Home tab is available.
Tab Toolbar	These components include the back and forward arrows, which function the same as in any standard browser as well as various viewing options that allow you to resize the panel dimensions to whatever best suits your needs. This toolbar also contains menus and buttons that are specific to the selected tab.
Page body	The Page body varies, depending on the tab that you are viewing. The Home page consists of labels that identify the product, case, functionality available, and sections that identify categories of EnCase components and contain links to the features or actions belonging to each category.

NEW CASE

To start a new case, click on the **New Case** link.

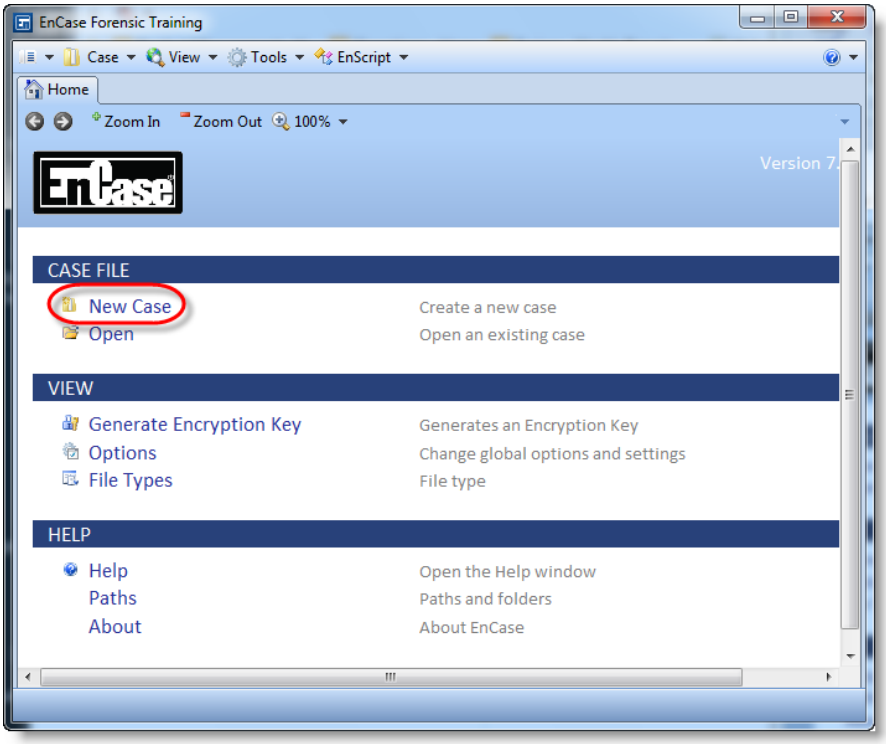

Figure 3-3 New case

The Case Options dialog box will appear, allowing for the selection of the Base case and evidence cache folders for the new case. By default, paths to your user directory are displayed. The investigator should change these paths to those specific to the case in order to segregate case data.

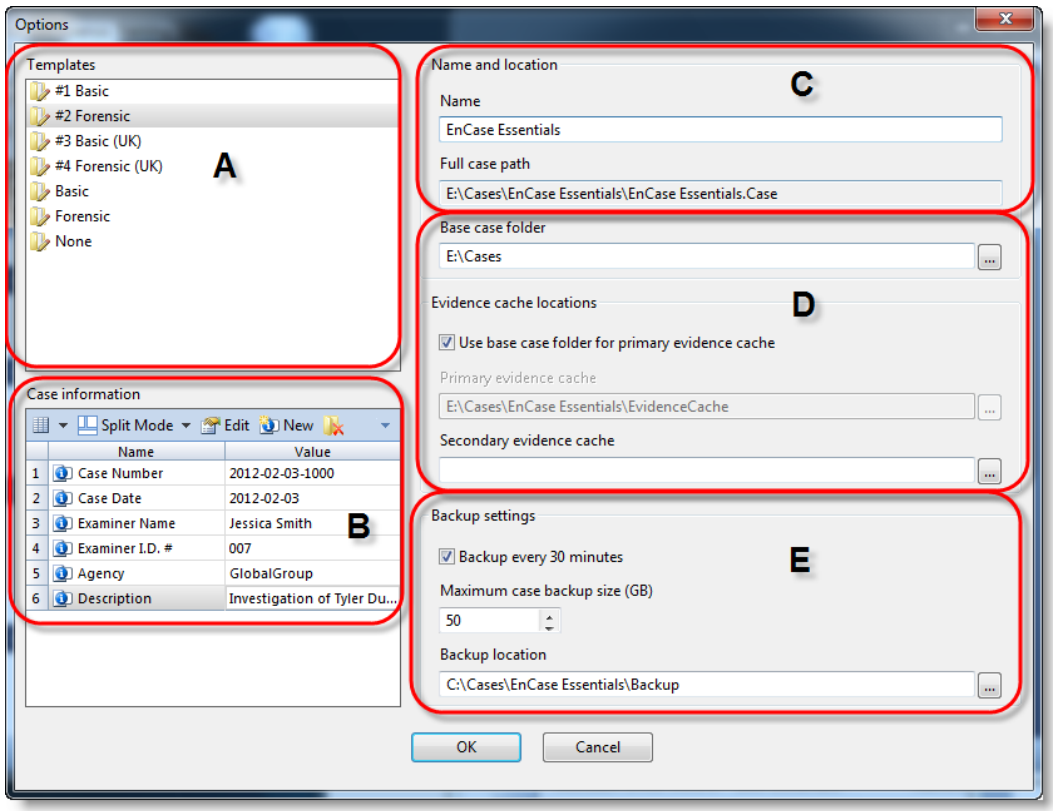

Figure 3-4 Creating a new case

A. Case Template

When you create a new case, you will see a list of available templates (these are `.CaseTemplate` files). EnCase supplies several predefined templates whose names appear in this box along with any saved templates.

To select a template:

Click on a name from the case **Templates** list to select it. In the previous figure, the **#2 Forensic** template is selected.

Although you can configure a new case completely from scratch, Guidance Software recommends using a template as it simplifies the case-creation process. Each case template contains a uniquely configured set of the following:

- Case info items with default values
- Bookmark folders and notes
- Tag names
- Report template
- User-defined report styles

You can also create your own templates by saving any case as a template. Afterwards, the new template will appear in the Templates list and will be available for future use. If you intend to create a number of cases with a similar structure, it makes sense to save one of them as a template and use it to generate the other cases.

B. Case Information

Case info – Case info items are user-configurable, name-value pairs that document information about the current case. These items are primarily used to insert user-definable information into a report. To update a value, double-click on the row.

To create case info items, use the **New** button above the table to generate as many name-value pairs as you need.

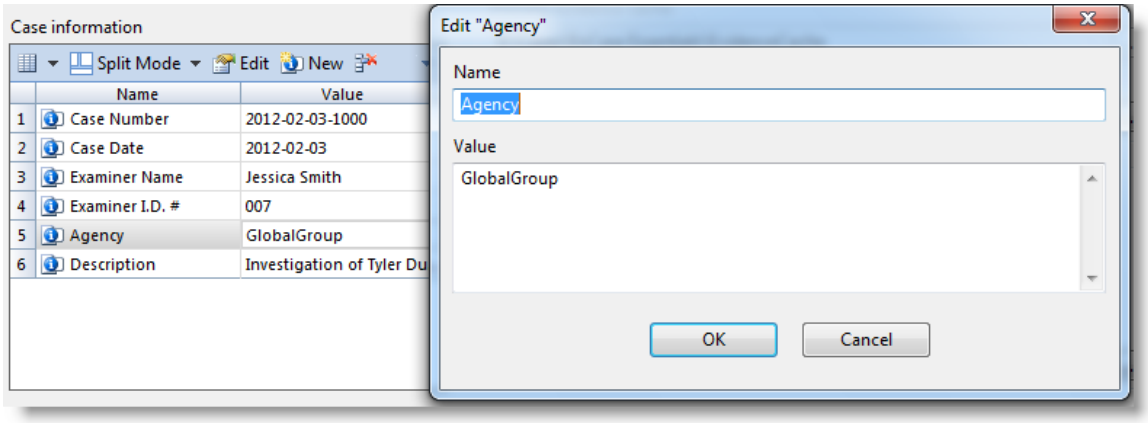

Figure 3-5 Case Information for Report

C. Case Name

Name –Text string you enter to identify the case file. In EnCase v7, a case is no longer contained within a single file, but is stored within a folder containing many components. The name specified in this field will be used to name the case folder as well as components contained within that folder.

Full Case Path – The folder in which the case file is stored. This field is not writable.

D. Case Folders

Base Case folder – This is the location where the case folder will be created. By default EnCase uses a folder under your `My Documents` folder.

Primary evidence cache – EnCase v7 uses cache files to speed up application responsiveness, enhance stability, and provide scalability across large data sets. The primary evidence cache folder is the location where EnCase will save and/or access these files. Cache files may be created in advance through the Evidence Processor and you can simply point to a folder that contains this data. Although there is an evidence cache for each device in a case, the evidence cache does not need to be stored with the evidence files. If cache files have not been created for a device, they will be stored in this folder when the Evidence Processor is run.

Secondary evidence cache – EnCase allows you to specify a secondary location where a previously created evidence cache can be found. This allows you to specify a folder on a network share or other location where cache files may be stored. Unlike the primary evidence cache folder, EnCase will only read previously created files from this location. All new cache files will be stored in the Primary evidence cache folder.

E. Backup settings

Backup every 30 minutes – By default, EnCase will back up your case every 30 minutes.

Since backups can take a significant amount of time, they occur in a background thread, allowing you to continue with your work.

Concerning the case backup:

- Can be canceled at any time, like any other background thread
- Stops silently if the case is closed
- If interrupted, continues at a later time, resuming where it left off (not copying the unchanged files again)
- Runs on this schedule:
  - Every 30 minutes while a case is open
  - When a case is opened, if that case has not been opened for more than 30 minutes
  - 30X minutes after the case is opened, if the case has not been opened for X minutes where X is less than 30
- Stops if the Evidence Processor is running
- Does not run if the Evidence Processor is already running
- Disables the automated backup timer while running

Maximum case backup size (GB) – By default, EnCase will allocate a maximum of 50GB of space for the case backup files

Backup location – This is the location where the backup files saved. By default EnCase uses a folder under your `My Documents/CaseBackup` folder.

The last backup folder location, maximum amount of disk space, and enable/disable backup are saved in the global settings and are automatically populated when you create a new case.

Click **OK** to apply the case options. To aid you, these constraints are checked:

- If you create a case with backup disabled, a dialog asks if you are sure you want to disable backup for this case.
- A warning displays if the backup location is not a valid path
- Choosing a backup and case folder on the same drive letter displays a warning, asking if you are sure you want to back up the case on the same drive as the case.
- Choosing a backup and evidence folder on the same drive letter displays a warning, asking if you are sure you want to back up the case on the same drive as the evidence cache.

The **Home** tab will then display a page for this particular case with the case name displayed at the top. This case page lists hyperlinks to many common EnCase features and you can use it as the main landing page for this case. You are now ready to begin building your case.

Working with Cases

Use the **Case** menu and the **Case** selections on the Case Home page to work with the parameters of and perform actions on your case.

Following are a list of basic operations for working with a case. Use the menu items on the **Case** menu and the links beneath the Case section on the Case panel for these operations.

Case Selections

Save (Ctrl-S)	Saves the current case file. The default suffix for a case file is *.Case; the default suffix for a backup case file is *.cbak.
Save As...	Used to save and rename the current case file or create a copy of the case file with a different name.
Create Package (Ctrl-P)	Creates a case package file for portability with the evidence.
Case Backup	Accesses the Case Backup dashboard.
Save As Template...	Used to save the case as an EnCase template to use with new cases. The extension for a case template file is *.CaseTemplate.
Close	Closes the active case file.
Open...	Opens an existing case file. (Note that you can have more than one case file active at a time.)
New Case...	Opens the Case Options dialog so that you can create a new case file.
Options...	Allows you to edit the Case Options for the active case.
Hash Libraries...	Displays the Hash Libraries dialog, which provides a list of hash libraries and hash sets used in the current case and allows you to change libraries or enable and disable hash libraries and sets.

If you need to update the Case options later, they are available under the Case menu.

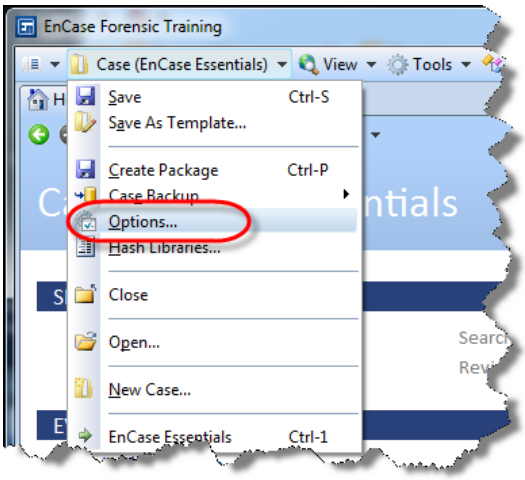

Figure 3-6 Accessing case options

Make any required changes to the case information and click **OK**.

NOTE: You cannot change the information contained in the Name or Case path fields; this information in displayed for reference purposes only and is read only.

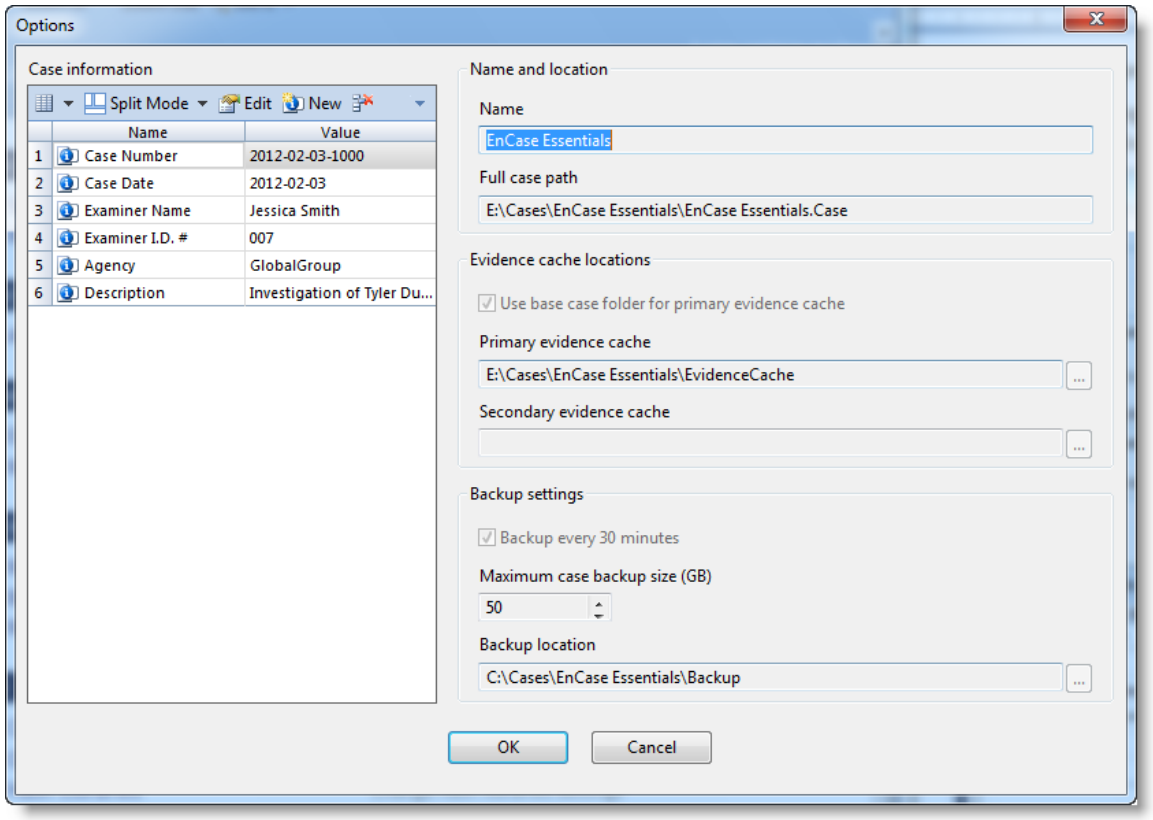

Figure 3-7 Case Options

Saving Your Case

Click on the **Save** link on the Home page to save your case.

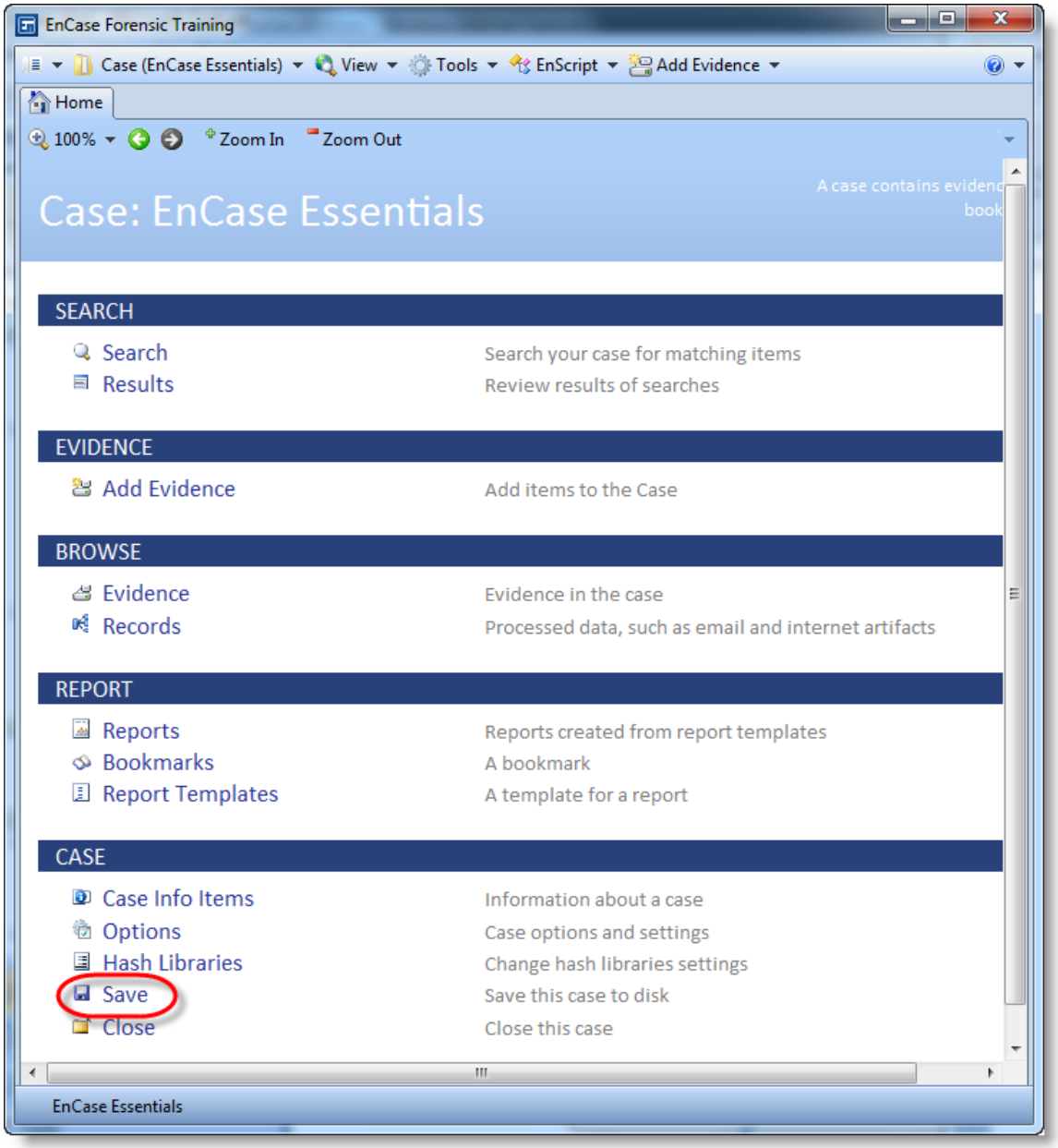

Figure 3-8 Case Home

Notice that several folders were created in the case folder:

- **EvidenceCache** – Storing cache files and containers for processed evidence
- **Email** – E-mail processing folder
- **Documents** – Default folder for documents
- **Searches** – Default folders for saving Search queries
- **Export** – Default folder for exporting evidence
- **Tags** – Tags storage
- **Temp** – Default temporary folder for file viewing

Later, other folders will be created during process:

- **CorruptPictures** – Holds corrupt pictures during the thumbnails creation process
- **Results** – Stores the results of index queries

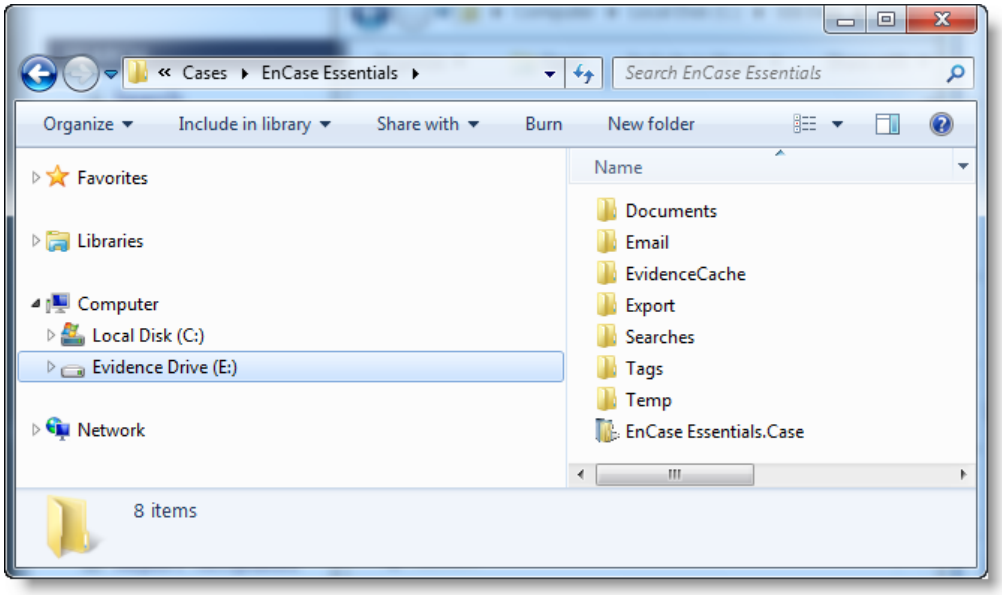

Figure 3-9 Default case folders

Create a folder named "LocalEvidence" and copy the TDurden.Ex01 evidence file from the EnCase Essentials OnDemand distribution website into the folder.

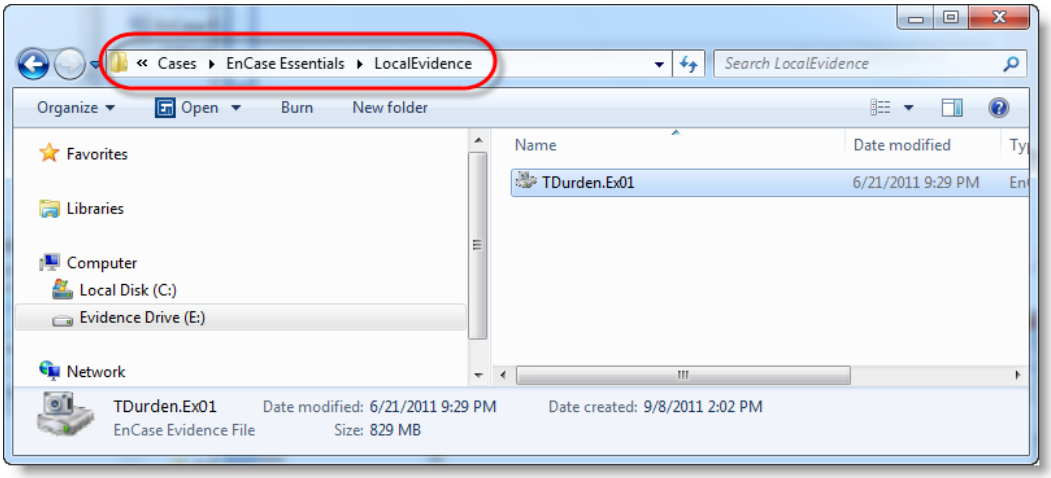

Figure 3-10 EnCase Essentials evidence

CASE BACKUP DASHBOARD

The Case Backup dashboard is the management interface for interacting with all backups for a particular case. The dialog shows a list of all available case backups in a tree format and sorts them by type (types are described in the following section).

To modify case backup options, click **Case→Case Backup→Use Current Case**.

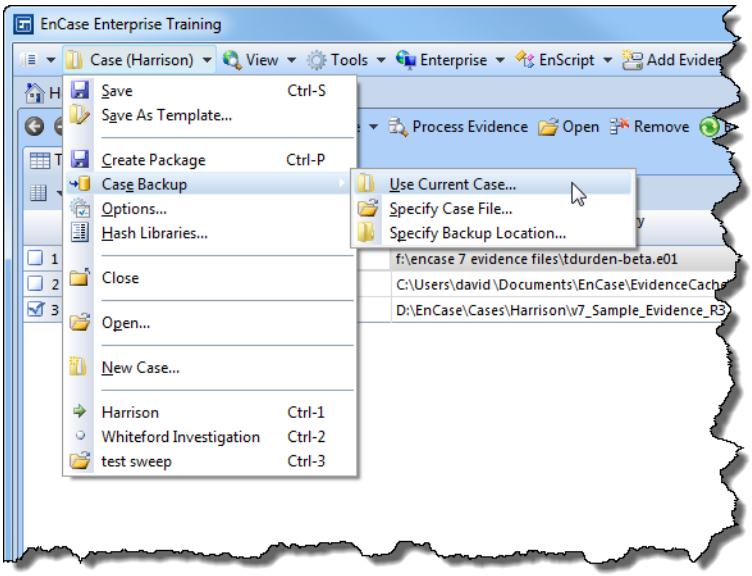

Figure 3-11 Case Backup options

The Case Backup menu opens a backup folder location and displays the case backup dashboard. The dashboard's input is the folder location, which comes from three possible locations. The Case Backup menu allows you to obtain the backup folder location from:

- **Use Current Case**: Uses the backup folder location from the currently open and active case
- **Specify Case File**: Reads from and uses the backup folder location from an unopened case file through an open file dialog
- **Specify Backup Location**: Uses the backup folder location specified by the user through a folder dialog

For each case backup, the dashboard displays these columns:

- Name
- Created
- Size (in bytes, KB, MB, GB, etc.)
- Custom name (if available)
- Comment (if available)

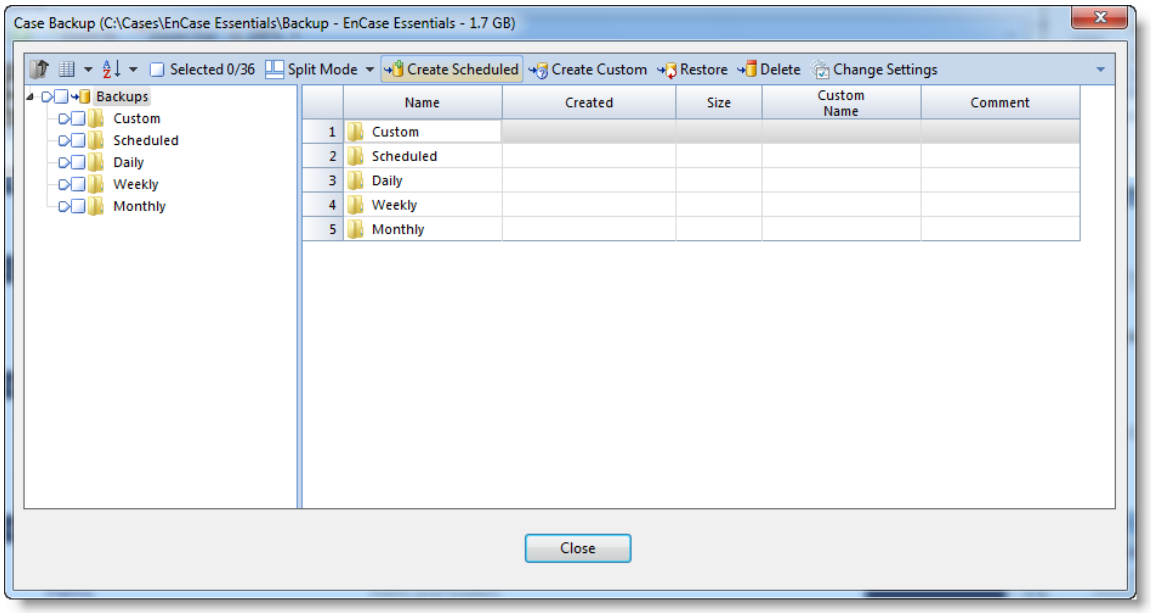

Figure 3-12 Case Backup dashboard

The dashboard shows a list of all available case backups in a tree format and sorts them by type. Daily, weekly, and monthly backups are created as a result of aging scheduled backups. The backup types and their aging attributes are:

- **Custom**: This is a user-created backup where you can provide a custom name and comments. Custom backups are retained until explicitly deleted.
- **Scheduled**: A scheduled backup is created when you open a new case or schedule a backup manually using the **Create Scheduled** option.
- **Daily**: Every scheduled backup that is closest to that day's local midnight time is copied and stored as a daily backup.
- **Weekly**: Every daily backup that is closest to that week's Sunday local midnight time is copied and stored as a weekly backup.
- **Monthly**: Every daily backup that is closest to that month's first day at local midnight time of the next month is copied and stored as a monthly backup.

By default, the database stores a maximum of:

- 48 scheduled backups
- Seven daily backups
- Five weekly backups

Monthly backups are kept until the maximum size allowed is exceeded. Oldest monthly backups are deleted to stay under the maximum size allowed.

USE CURRENT CASE

1. Click **Case→Case Backup→Use Current Case** and the dashboard displays.
   - To create a scheduled backup click **Create Scheduled**.

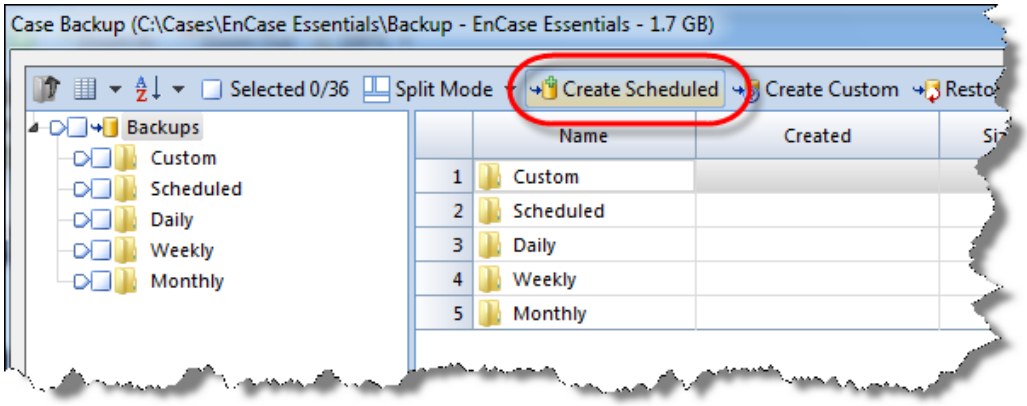

Figure 3-13 Backup – Current Case

2. The Create Scheduled Backup dialog displays.

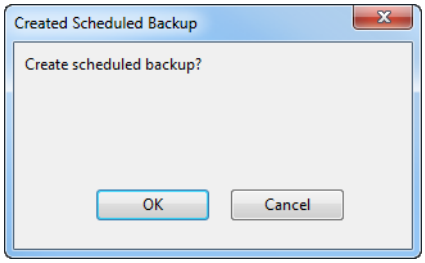

Figure 3-14 Case Scheduled Backup

3. Click **OK**. The Created Scheduled Backup progress bar displays.

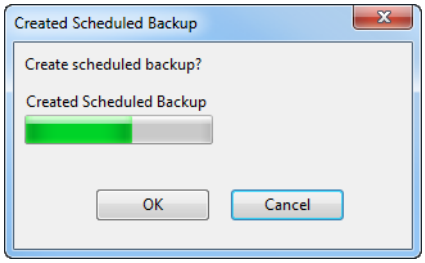

Figure 3-15 Create Scheduled Backup

4. After the backup is scheduled, the Create Scheduled Backup dialog closes. To verify that the backup was scheduled, click the **Scheduled** folder in the Backups directory.

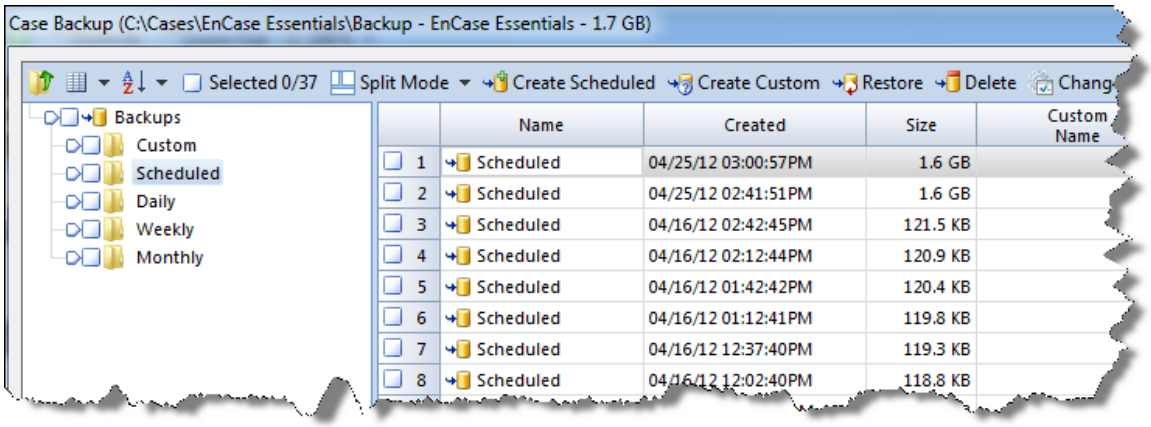

Figure 3-16 Scheduled Backup

CREATE A CUSTOM BACKUP

1. Click **Case→Case Backup→Use Current Case** and the dashboard displays.
   - To create a custom backup click **Create Custom**.

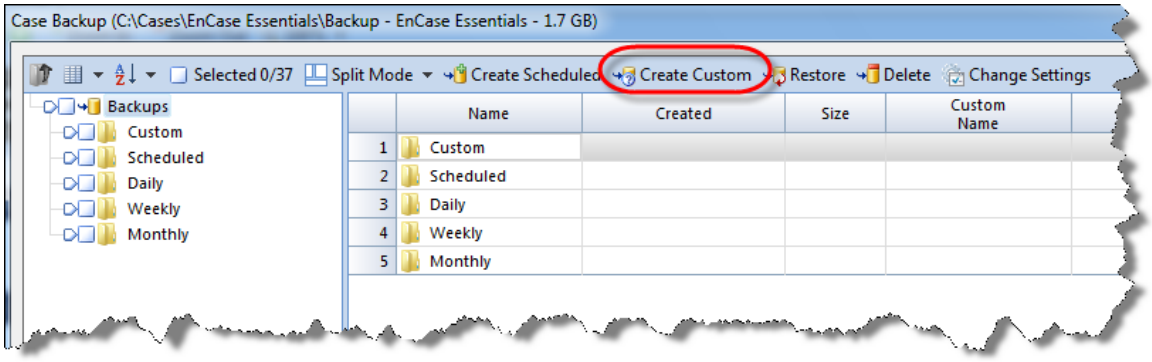

Figure 3-17 Create Custom Backup

2. The Create Custom Backup dialog displays.

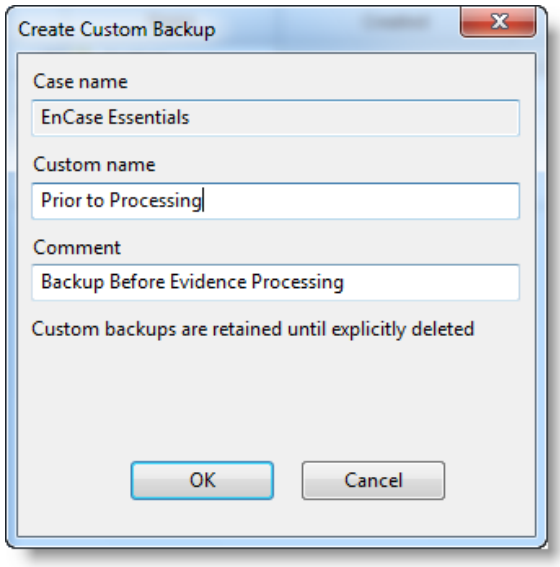

Figure 3-18 Create Custom Backup Dialogue

3. Enter a custom name and, if desired, a comment, then click **OK**.
4. To verify that the custom backup was created, click the **Custom** folder in the Backups directory.

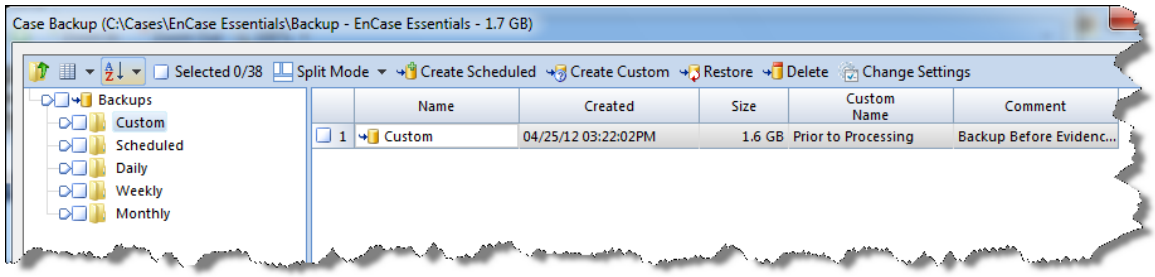

Figure 3-19 Custom Backup

SPECIFY CASE FILE

Specify Case File reads from and uses the backup folder location from an unopened case file.

1. With no case open, click **Case→Case Backup→Specify Case File**.

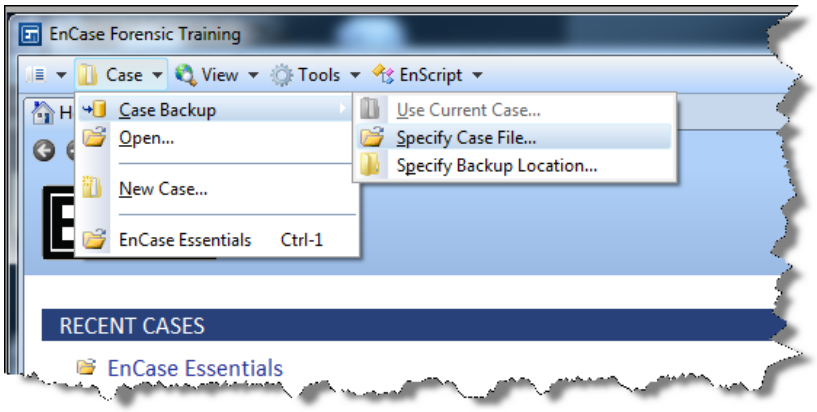

Figure 3-20 Specify Case File…

1. The **Open File** dialog displays.

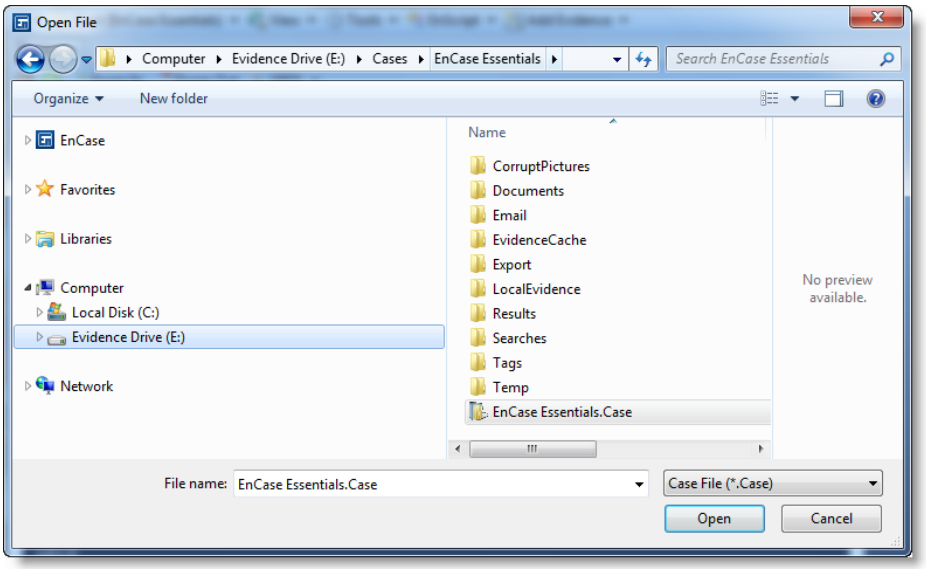

Figure 3-21 Open Case File

2. Select the case file you want then click **Open**. The dashboard displays for the case file you selected.

3. If you desire to restore a backup, select a backup file and click **Restore**.

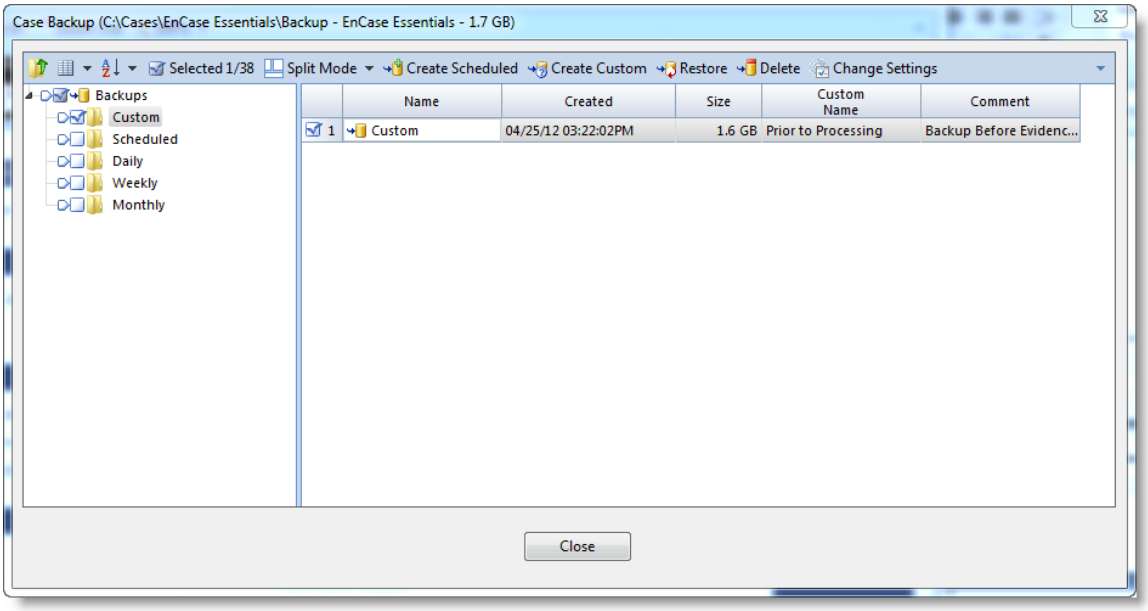

Figure 3-22 Restore Case Backup

SPECIFY BACKUP LOCATION

To specify a backup location click **Case→Case Backup→Specify Backup Location**.

1. The Browse for Folder→Case Backup Location dialog displays.

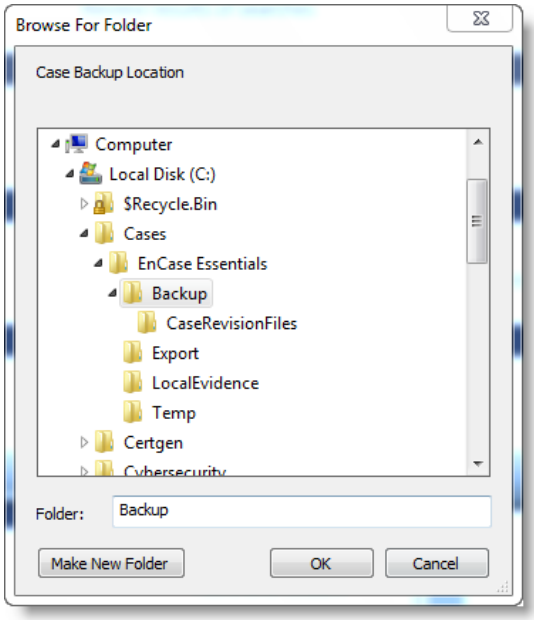

Figure 3-23 Browse for Folder

2. Navigate to the location you want for the backup, then click **OK**.
3. The Case Backup Folder is displayed. Click **OK**.

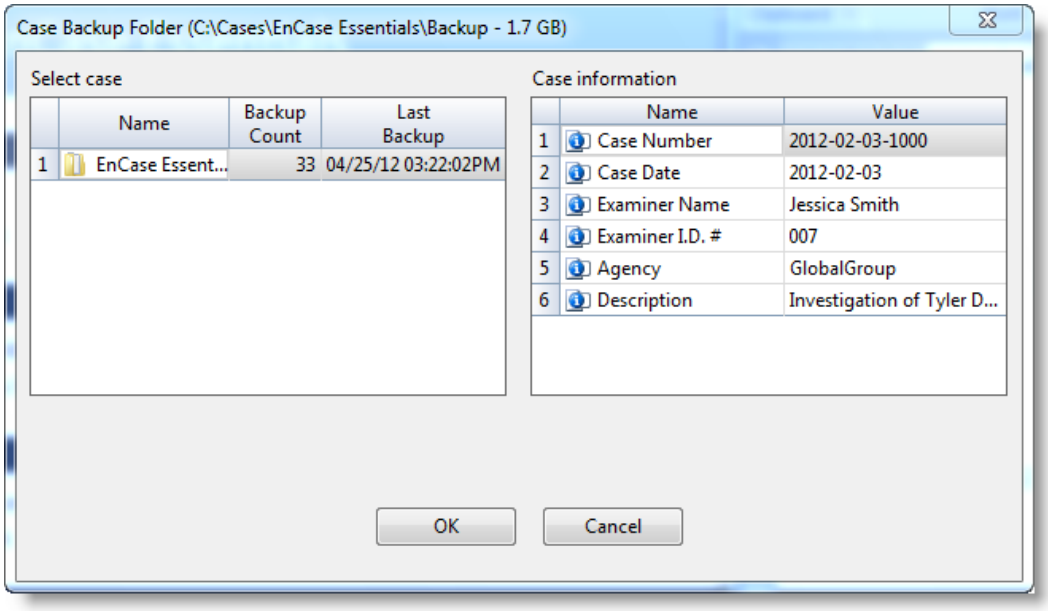

Figure 3-24 Confirm case backup folder

RESTORING FROM BACKUP

Restoring from backup restores the following types of data:

- Case file
- Everything in the case folder, except:
  - Export folder
  - Temp folder
  - Evidence files (.E01, .L01, .Ex01, and .Lx01)
- Primary evidence cache (only those evidence caches referenced in the case)
- Secondary evidence cache (only those evidence caches referenced in the case)
- Dates, times, and sizes for all files.

How to Restore from Backup

Click **Case→Case Backup→Specify Case File** or **Specify Backup Location**.

1. With no case open, select the case you want to back up then click **Open** to display the dashboard
2. In the dashboard, select the folder in the Backups directory, which contains the backup you want to restore.
3. Blue-check one (and only one) backup then click **Restore**.

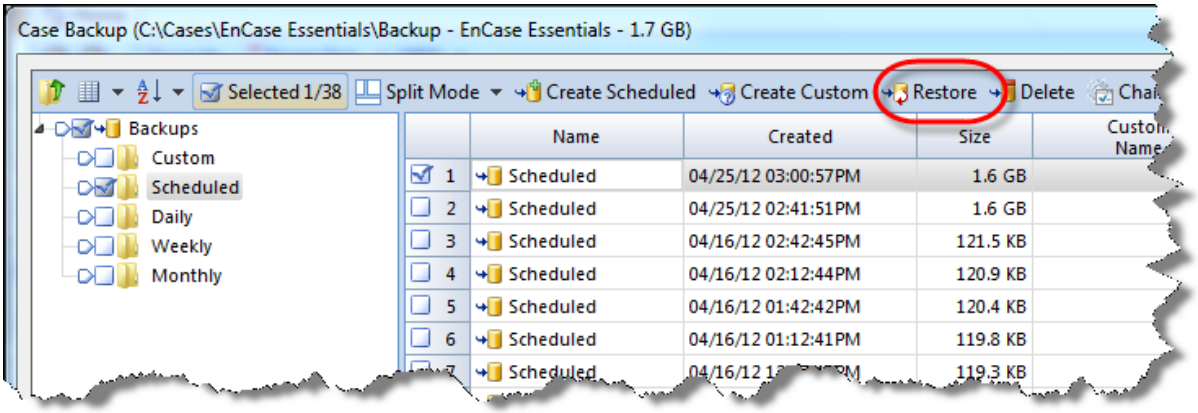

Figure 3-25 Restore backup

4. The Restore Backup dialog displays. Click either **Restore to original case locations** (default) or **Restore to new locations**, then click **Next>**.

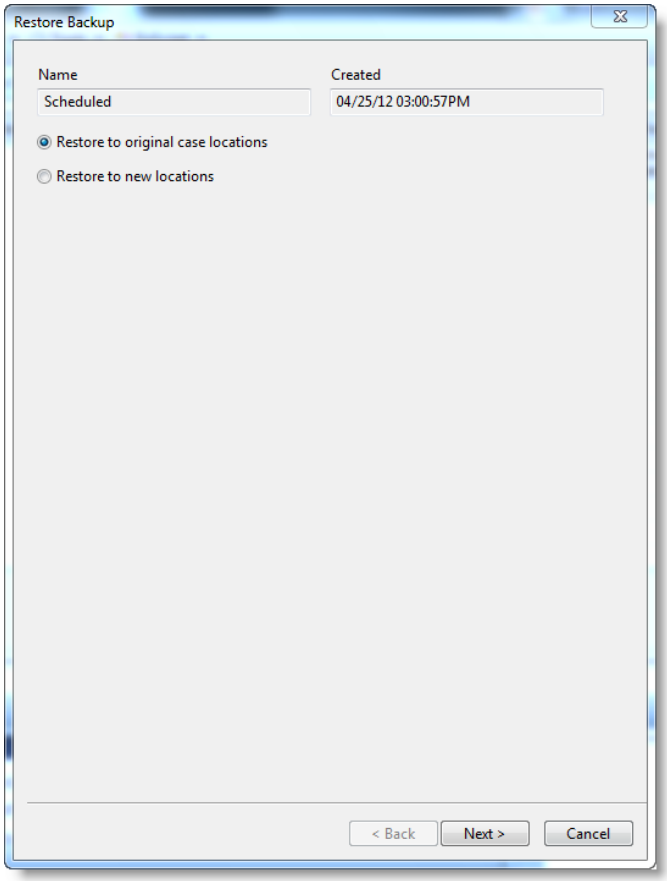

Figure 3-26 Create Custom

- If you click **Restore to original case locations**, the Name, Location, and Full Case Path fields populate automatically and you cannot edit them. All other options are disabled.
- if you click **Restore to new locations**, the Name, Location, and Full Case Path fields populate and you cannot edit them. However all other options are enabled, and you can change any of them.

5. When you are done, click **Finish**.

NOTE: Restoring will overwrite the contents of the selected Case directory.

DELETING A BACKUP

To delete a backup go to the dashboard using any of the options in the **Case→Case Backup** drop-down menu. From the Backups directory, open the folder containing the backup you want to delete.

1. Blue-check the backup or backups you want to delete, then click **Delete**.

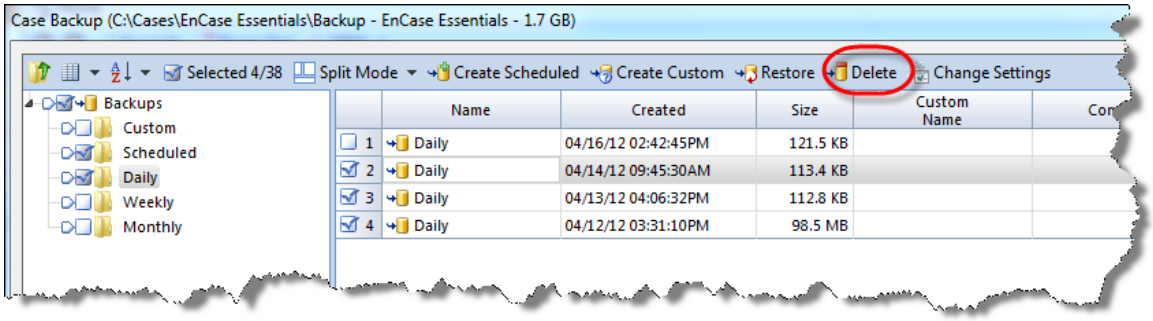

Figure 3-27 Delete selected backups

2. A warning message displays:

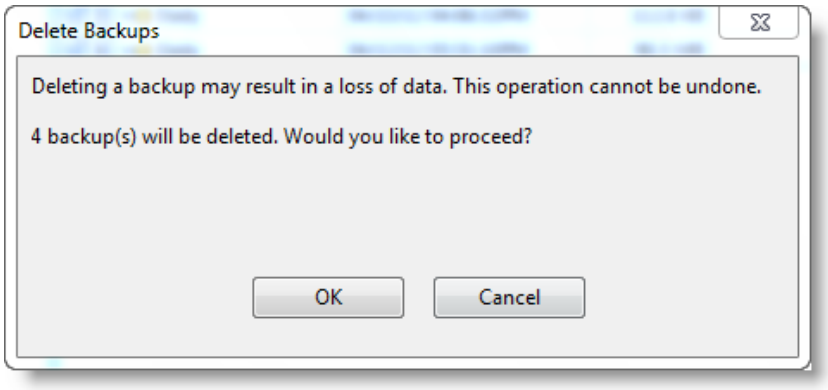

Figure 3-28 Create Custom

3. To continue, click **OK**. The selected backups are deleted.

CHANGING CASE BACKUP SETTINGS

To change case backup settings, a case must be open:

1. Click **Case** > **Case Backup** > **Use Current Case**
2. On the dashboard, click **Change Settings**
   - The Change Case Backup Settings dialog displays

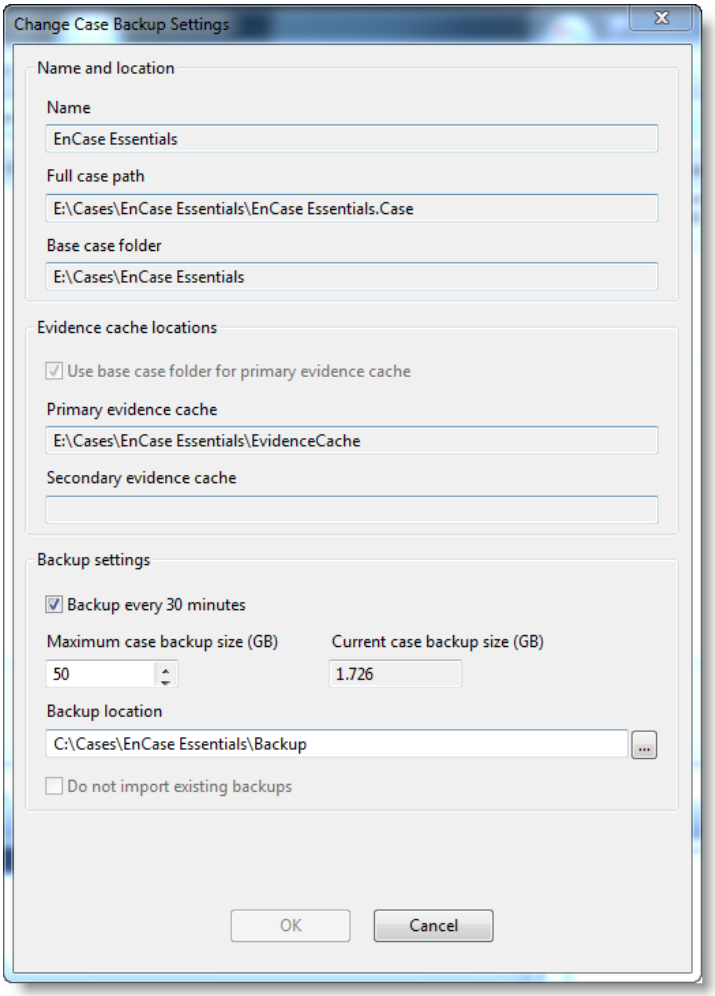

Figure 3-29 Create Custom

3. You can make these changes:
   - Enable or disable **Backup every 30 minutes**
   - Maximum case backup size (GB)
   - Backup location
4. Make the changes you want, then click **OK**

ENCASE GLOBAL CONFIGURATION SETTINGS

EnCase configuration settings that are global may be found by selecting **Tools→Options…**.

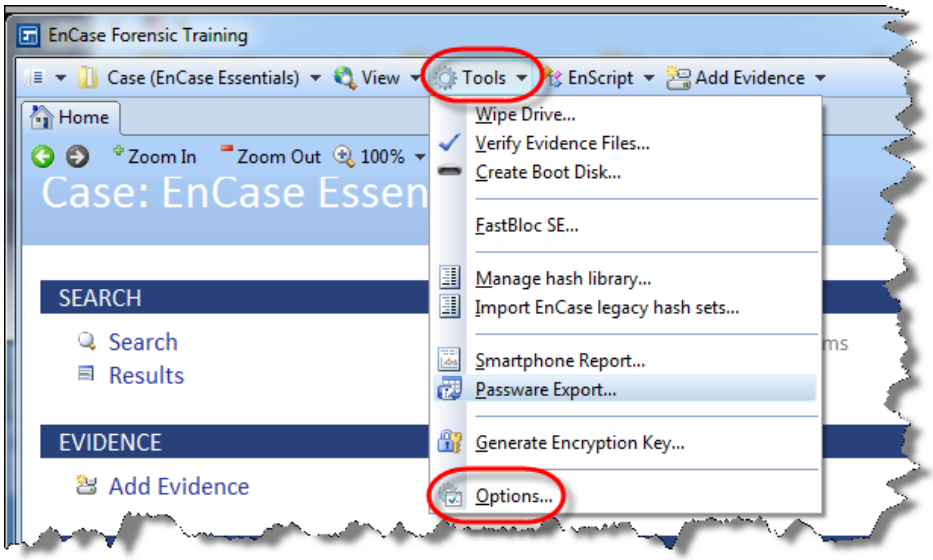

Figure 3-30 Global configuration settings available in the Options window

The **Options** tab can modify the EnCase core configuration

- The **Global** tab allows various features to be changed, including the Auto Save Feature, picture, and timeout options
- The **Date** tab allows you to set the format for date and time stamps
- The **NAS** tab contains all of the settings needed to enable the network authentication of the EnCase® dongle if on a server instead of the local machine
- The **Colors** tab provides the ability to set the color scheme for different elements of the EnCase® interface
- The **Fonts** tab can alter screen fonts typically used for foreign-language support
- The **Shared Files** tab provides the ability to set the path to where user and application data is stored as well as the evidence and cache folders
- The **Debug** tab is utilized by EnCase users who experience abnormal shutdowns or program lockups and by those working with customer service to determine the nature of the problem

Global

This tab allows you to select options that establish the global-configuration settings for a case.

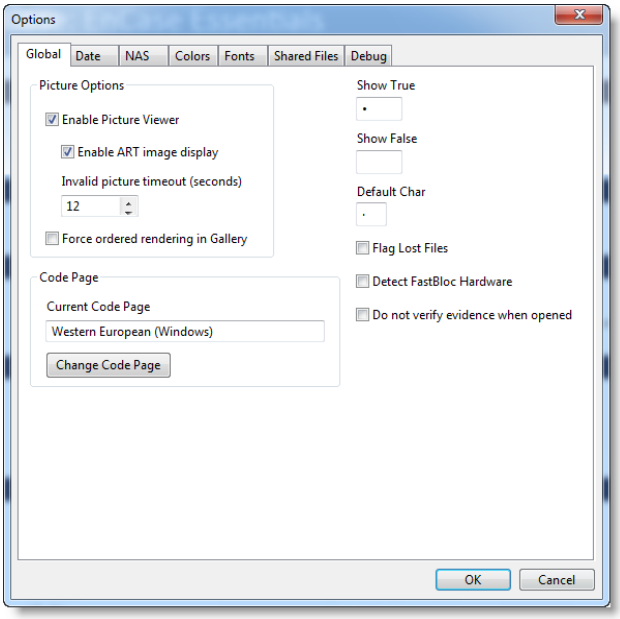

Figure 3-31 Options window – Global tab

Picture Options

- **Enable Picture Viewer** – This option allows pictures to be displayed in various views.
- **Enable ART image display** – This option provides you with the ability to not display files with these characteristics, which if corrupted, may cause an Internet browser like Internet Explorer to crash.
- **Invalid Picture Timeout** – This option enables EnCase to stop trying to read a corrupted image file. Instead the file is cached so that EnCase will not attempt to read it in the future. The default is 12 seconds.
- **Force ordered rendering in Gallery** – This new option for EnCase v7 was added to force the rendering of pictures in the Gallery to be in order from top left to bottom right. Checking this box forces the order rendering, while turning the option off makes EnCase render small pictures immediately and queue up the longer/bigger pictures.
    - This option is off by default because the Gallery view flows better from a user-interface perspective. However some users like to go to the Gallery view and scroll down one row at a time to see the pictures show up in order from left to right. This option was created for those users.

Code Page

- **Code Page** – Set the default code page for text viewing.

Additional Options

- **Show True / Show False** – This option defines the data that will appear in a Table column, indicating whether a condition is true or false. ***It is best to set these items to something that can be easily understood (such as "Yes" for true and "No" for false) rather than retain the default settings of bullet for "true" and blank for "false."***
- **Default Char** – The character used for non printable values, such as 00h, 01h, 02h, etc.
- **Flag Lost Files** – This option is unchecked by default, which means that lost clusters are treated as unallocated space, decreasing the amount of time required to access the evidence file through a case file. If this option is checked, EnCase will tag all lost clusters in Disk view (indicated by yellow blocks with a question mark). This option must be set before an evidence file is added to the case.
- **Detect FastBloc** – Detect legacy FastBloc for write blocking during evidence acquisition.
- **Don't verify evidence when opened** – Open evidence without verifying acquisition hash and CRC.

Date

This tab allows you to configure the date and time displays, including displaying the time zone on dates.

Date Format includes these options:

- **MM/DD/YY** (for example, 06/21/08)
- **DD/MM/YY** (for example, 21/06/08)
- **Other** enables you to specify your own date format
- **Current Day** displays the current date in the specified date format

Time Format includes these options:

- **12:00:00PM** uses a 12-hour clock for the time format
- **24:00:00** uses a 24-hour clock for the time format
- **Other** enables you to specify your own time format
- **Current Time** displays the current time in the specified time format

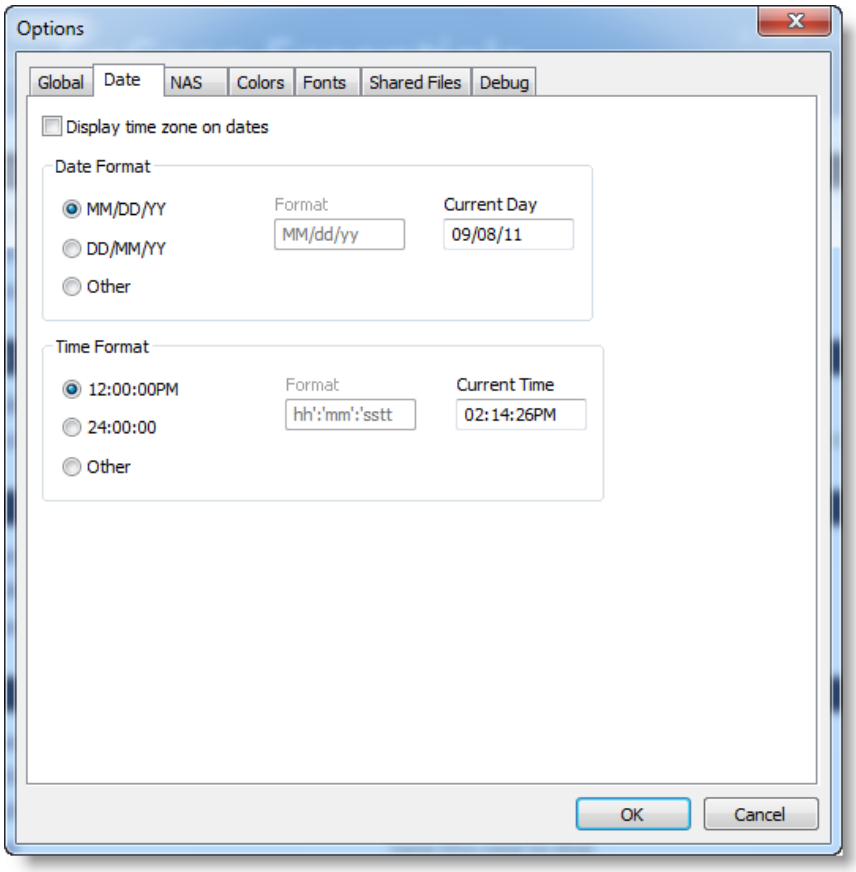

Figure 3-32 Options window – Date tab

NAS

NAS (Network Authentication Server) – This option allows multiple copies of EnCase to authenticate to a single hardware key. This is typically used in lab environments with multiple examiners and multiple copies of EnCase.

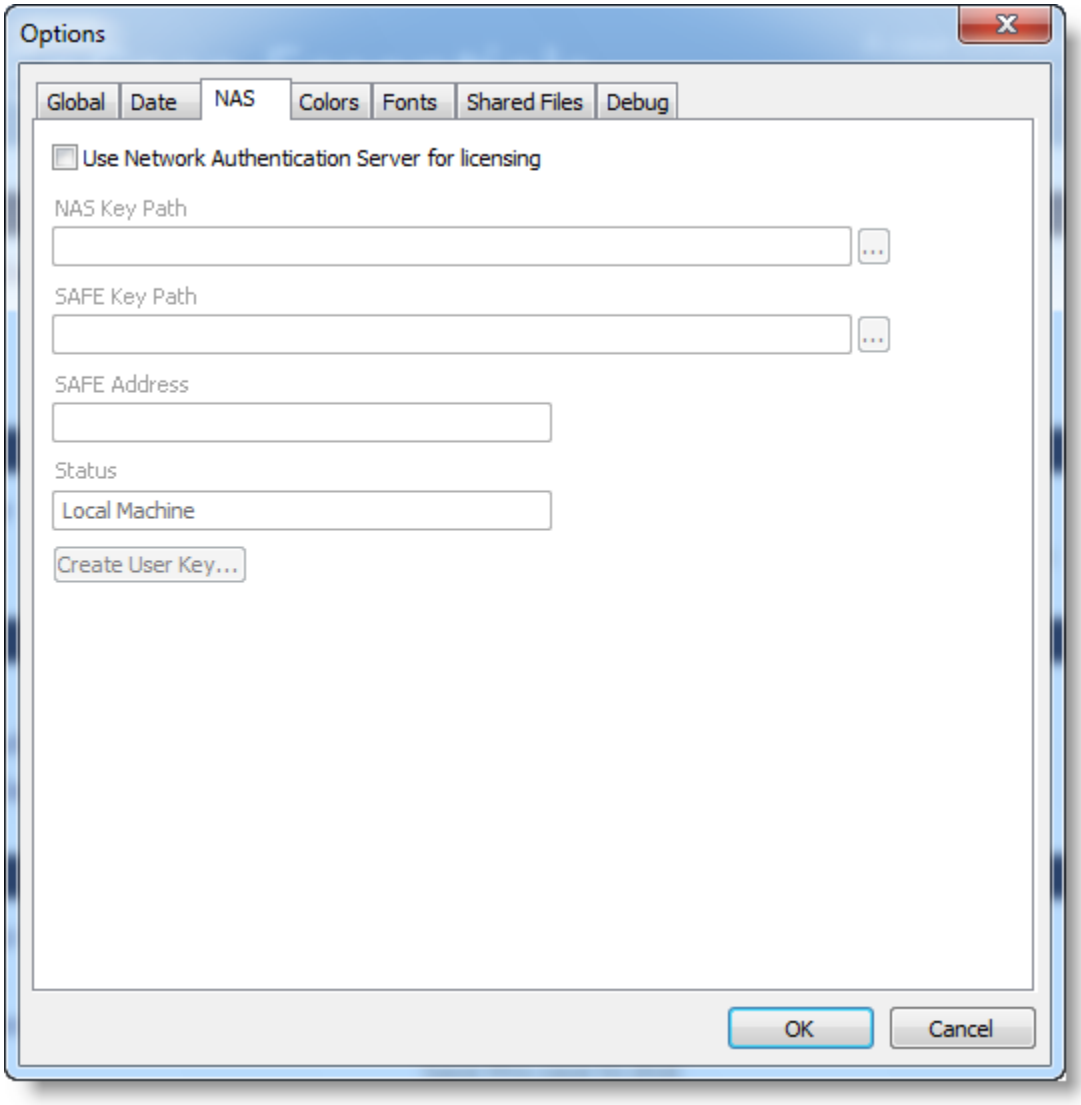

Figure 3-33 Options window – NAS tab

Colors

This tab allows you to change the colors for different elements of the EnCase interface.

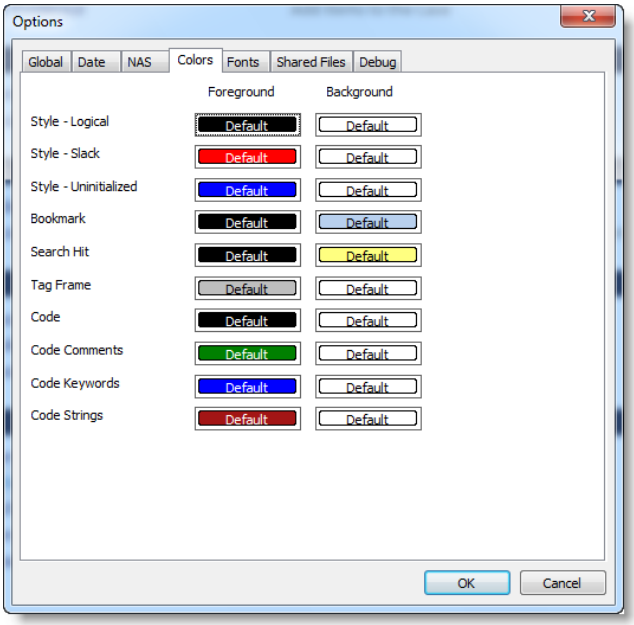

Figure 3-34 Options window – Colors tab

Fonts

This option allows you to alter fonts for viewing convenience and to accommodate the special font requirements of some foreign languages to display correctly.

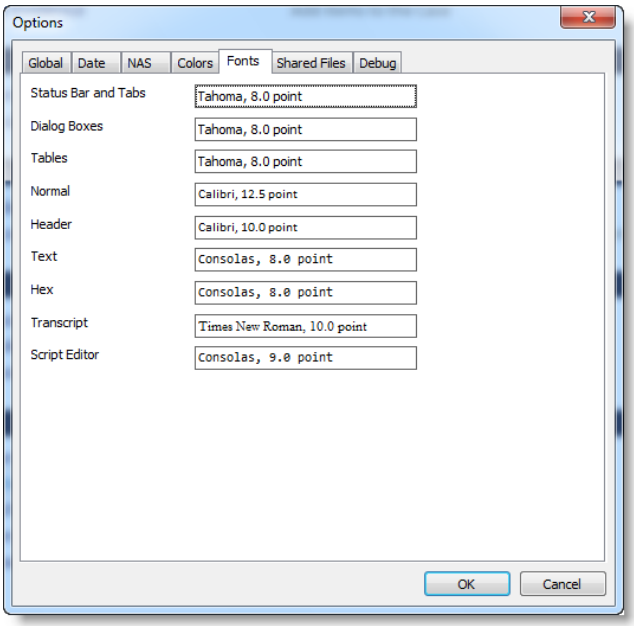

Figure 3-35 Options window – Fonts tab

Shared Paths

This option allows you to specify the folder for shared files, such as the filetypes.ini file, EnScript modules, filters, searches, conditions, and keywords.

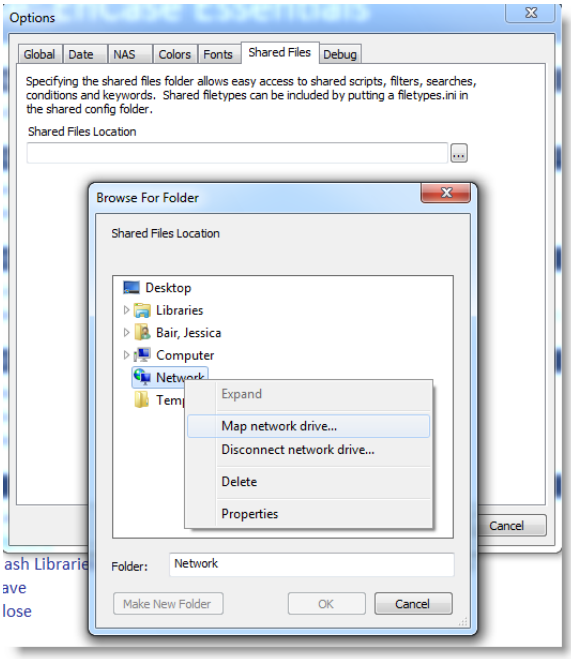

Figure 3-36 Options window – Shared Paths tab

Debug

This option is utilized by EnCase users who experience abnormal shutdowns or program lockups and by those working with customer service to determine the nature of the problem.

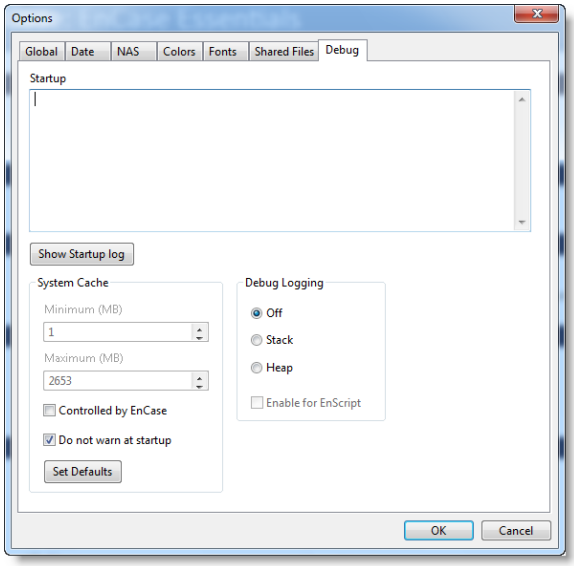

Figure 3-37 Options window – Debug Path tab

Hash Library and Analysis

Analyzing a large set of files, by identifying and matching the unique hash value of each file, is an important part of the computer forensics process. Using the hash library feature of EnCase v7, you can import or custom build a library of hash sets, allowing you to identify file matches in the examined evidence.

Computer forensics analysts often create different hash sets of known illicit images, hacker tools, or non-compliant software to quickly isolate known "bad" files in evidence. Hash sets are distributed and shared among users and agencies in multiple formats. These formats include NSRL, EnCase hash sets, Bit9, and others.

Until recently, the hash set standard to identify a file was the MD5 hash calculation. Large hash distribution sets, such as the NSRL set, are now distributed using the SHA-1 hash calculation. EnCase will offer continued support for MD5 hash sets from old versions of EnCase and other products as well as the new SHA-1 hash format sets.

EnCase uses an extensible format for hash sets that allows:

- Storing metadata along with the hash value in field form
- Support of MD5, SHA-1, and additional hash formats within the same file structure
- The association of tags with items in the hash set

Hashing Features

EnCase v7 contains several new and expanded hashing features:

- A versatile user interface for hash library management: you can create hash sets and libraries, import and export hash libraries, query hash sets, and view hash sets or individual hash items
- Hash libraries can contain multiple hash sets and each set can be enabled or disabled
- You can create as many hash libraries or hash sets as you want
- If a hash belongs to multiple sets, every match will be reported
- Each case can use up to two different hash libraries at the same time
- You can save individual hashes in a separate folder without placing them in a specific hash set or hash library (for example, you may want to retain a hash of an item for later use without committing it to a particular hash set or library)

WORKING WITH HASH LIBRARIES

A hash library is a folder containing the file-based, database-like structure in which EnCase stores hash sets.

To work with hash libraries, click on **Tools→Manage Hash Library…** on the Application Toolbar.

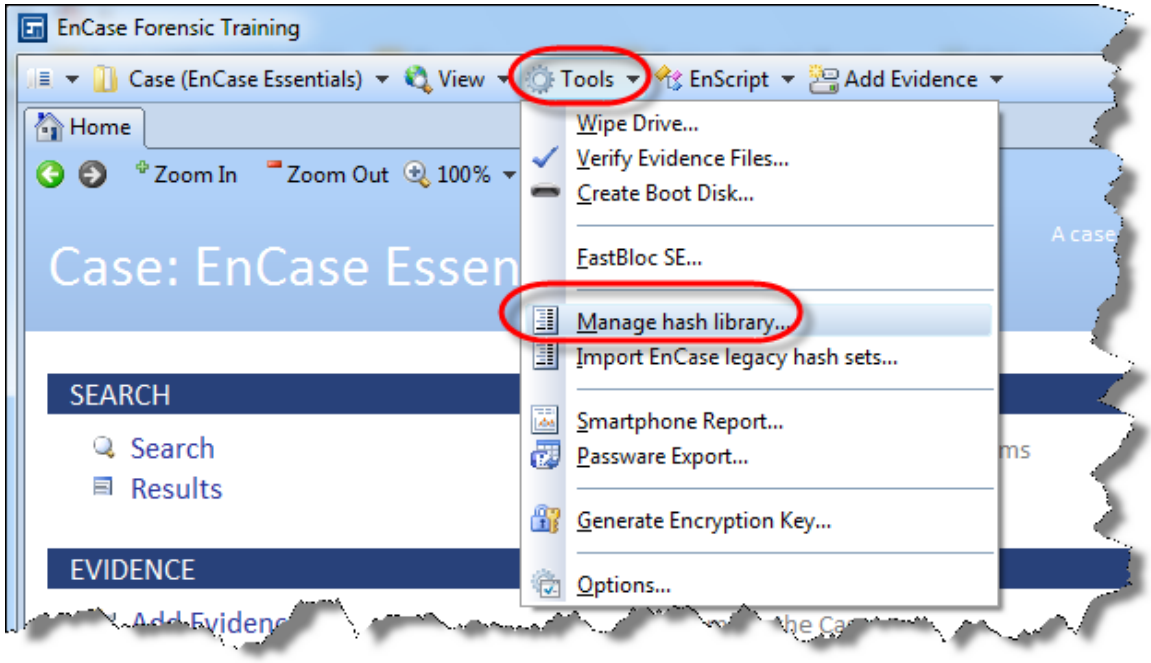

Figure 3-38 Managing hash library

Opening a Hash Library

From the Manage Hash Library dialog you can manage any existing hash libraries or create a new one. You use its toolbar to:

- Create a new hash library or edit an existing library
- Create new hash sets within a library or edit an existing hash set within a library
- Import and export hash sets from one library to another
- Query a hash library for a particular value

NSRL

You may wish to use a centralized hash library or one already created. Guidance Software, Inc. has converted the National Software Reference Library (NSRL) RDS 2.32 March 2011 (http://www.nsrl.nist.gov/Downloads.htm) hash set into the EnCase v7 format. You can obtain the converted hash set from the EnCase Support Portal (https://support.guidancesoftware.com/)

Download the converted NSRL hash sets from the EnCase Support Portal at:

https://support.guidancesoftware.com/

Place them in a directory that it easily accessible and usable, such as: `C:\Program Files\EnCase7\Hash Libraries\NSRL Hash Library`

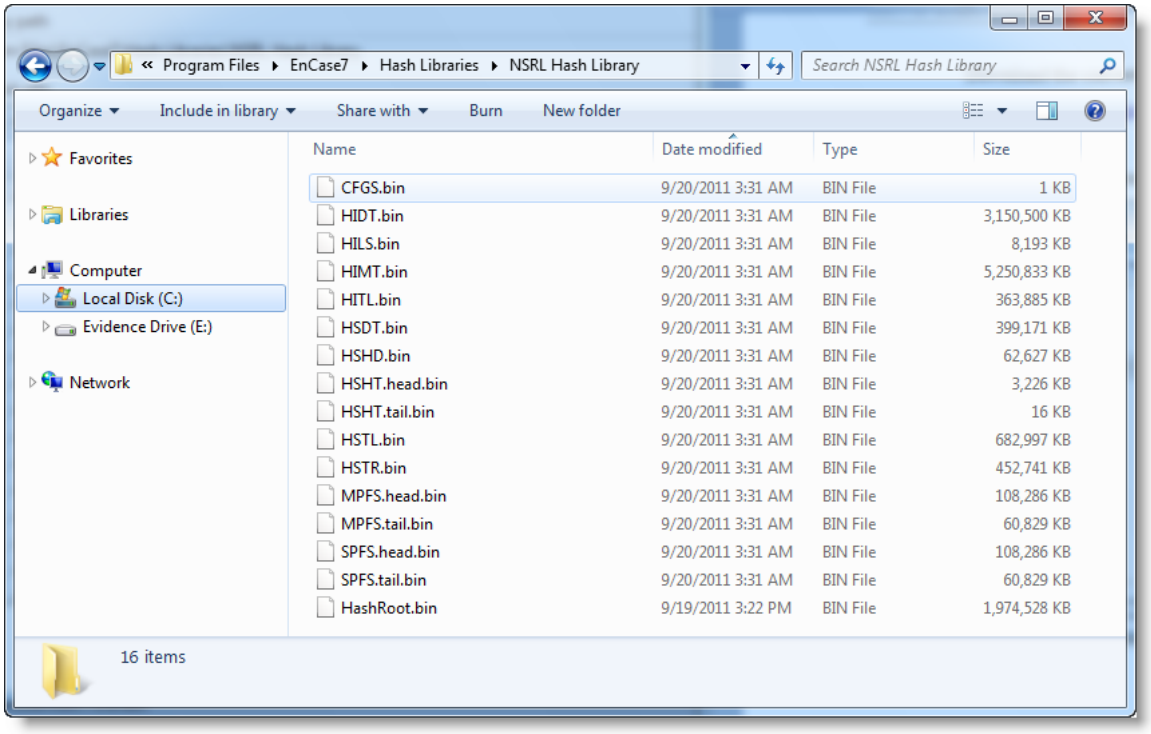

Figure 3-39 NSRL Hash Library

To open a hash library, click **Open Hash Library** and browse to the directory from the Manage Hash Library panel toolbar.

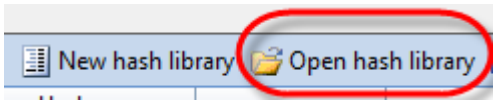

Figure 3-40 NSRL hash library

Browse to `C:\Program Files\EnCase7\Hash Libraries\NSRL Hash Library` and click **OK**.

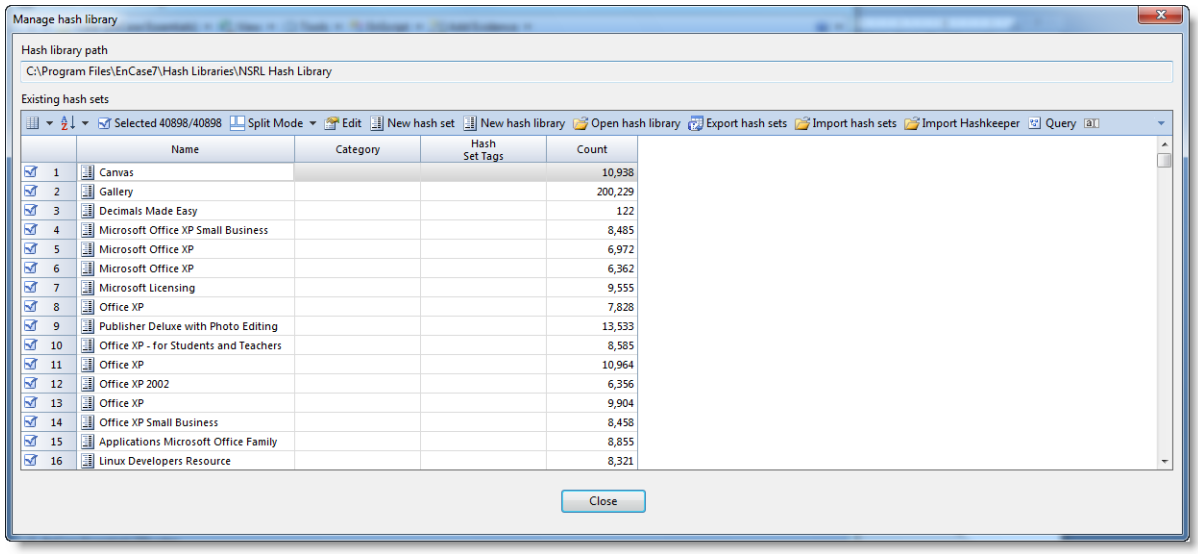

Figure 3-41 NSRL hash library in EnCase v7

MODIFYING CATEGORY AND TAGS FOR MULTIPLE HASH SETS

Rather than modifying each matching file set individually, you can now change the category and tags for multiple hash sets in a hash library.

In the Manage Hash Library dialog, blue-check the appropriate hash sets and then select **Edit Multiple**.

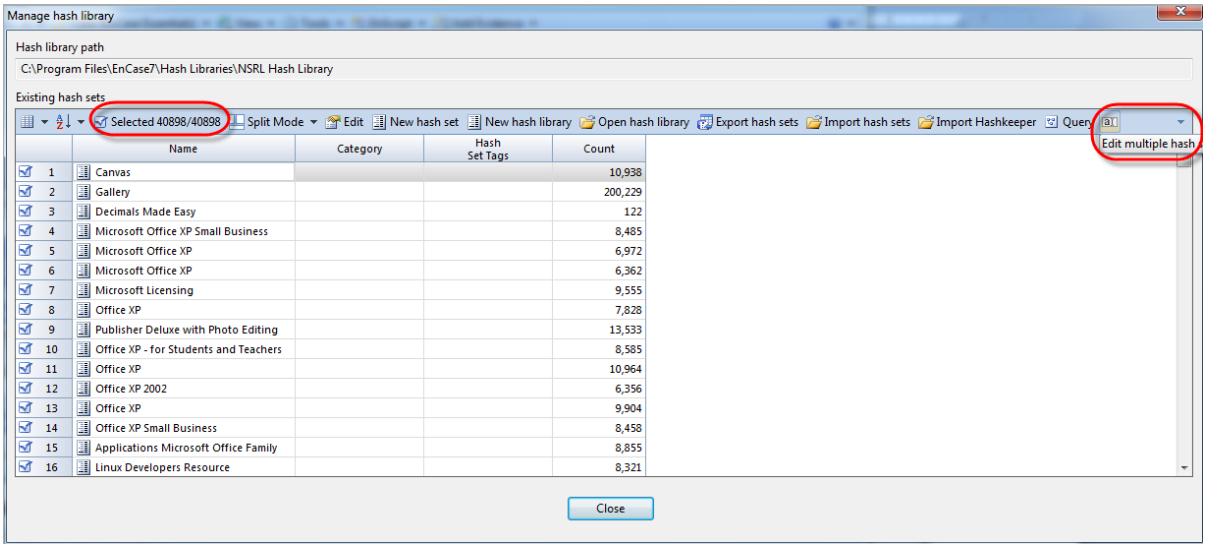

Figure 3-42 Edit multiple hash sets

The **Edit Multiple** dialog displays.

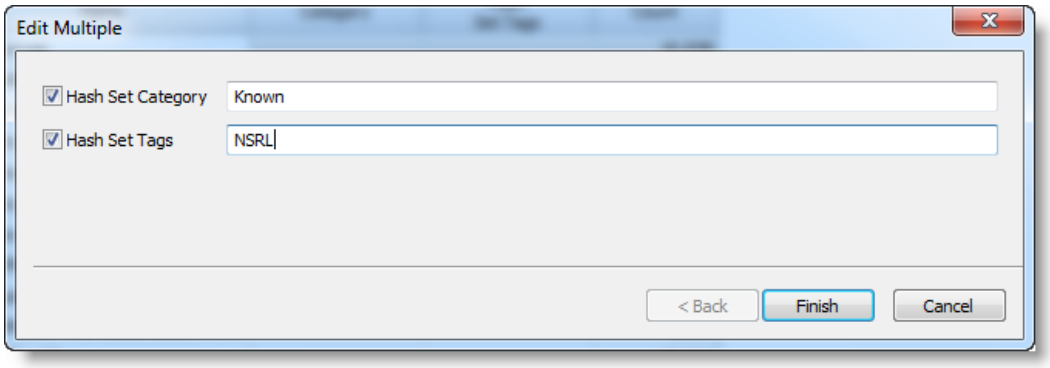

Figure 3-43 Edit Multiple hash sets – category and tags

Select whether you want to change the existing category or tag on the hash sets, then enter the new value in the text box.

NEW HASH LIBRARY

To create a new hash library, do the following within the Manage Hash Library interface:

1. On the Manage hash library panel toolbar, click **New hash library**

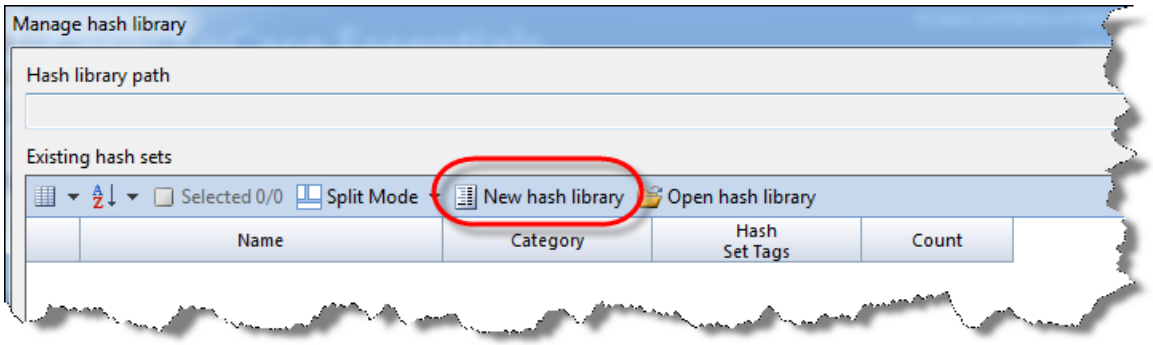

Figure 3-44 New Hash Library

2. Browse for a directory or create a new folder to hold the hash library

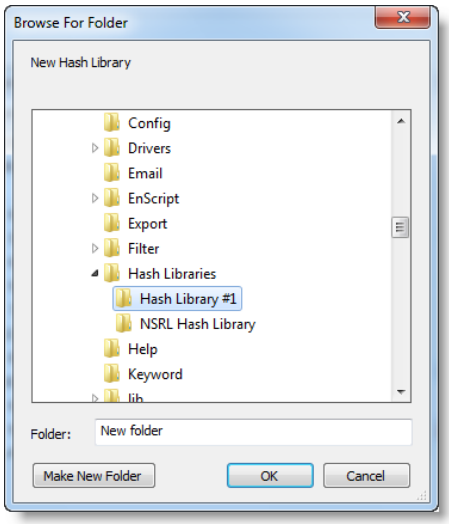

Figure 3-45 Browse for Hash Library

NOTE: *If you use an existing folder, it must be empty* (*otherwise, the contents of the folder will be deleted*).

3. Provide a name for the hash library (for example, "Hash Library #1")

4. Click **OK**

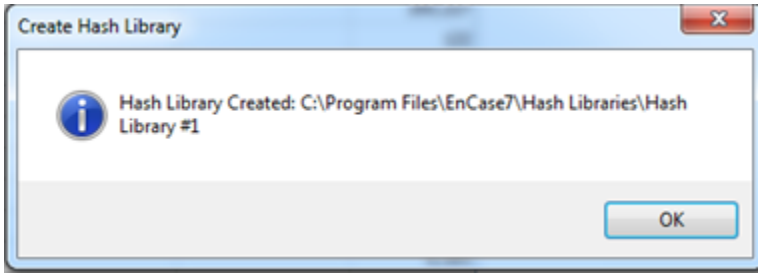

Figure 3-46 Hash library created

If you wish to import hash sets from another library, select **Import Hash Sets** from the toolbar.

You can then browse to a library and select individual sets to import, such as importing the NSRL library into your new Hash Library #1.

NOTE: **Ctrl+Space Bar** will select all of the hash sets.

Click **Finish** to import the hash sets; for now, click **Cancel**.

NOTE: ***With 11 GBs of hash sets, importing the NSRL RDS will take a long time.***

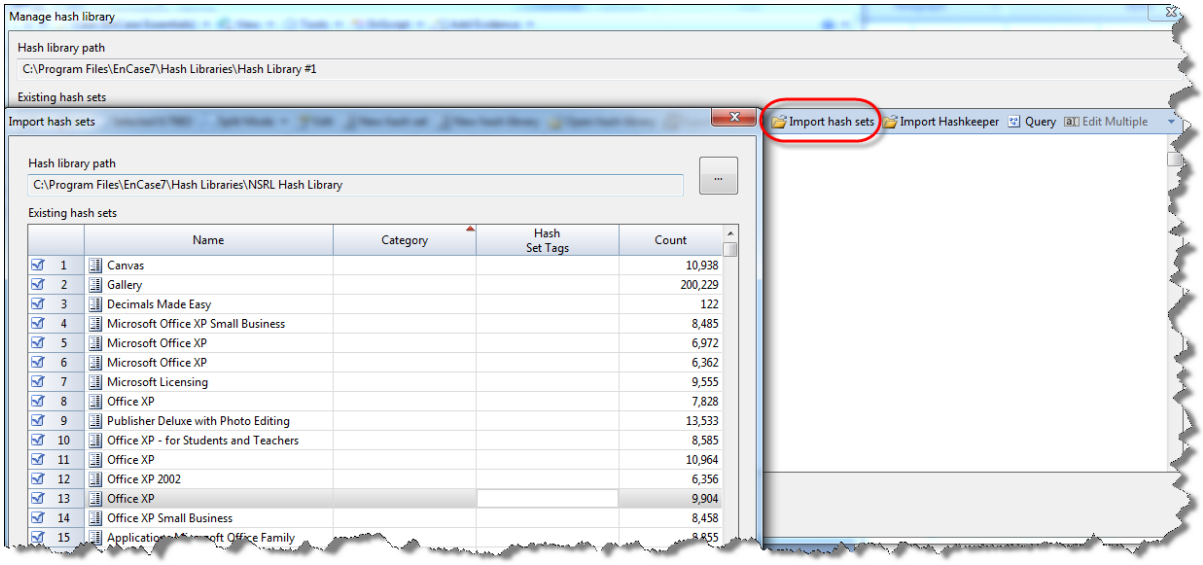

Figure 3-47 Import Hash Sets

ADD HASH SETS

We will add new hash sets to the current hash library after running the EnCase Evidence Processor.

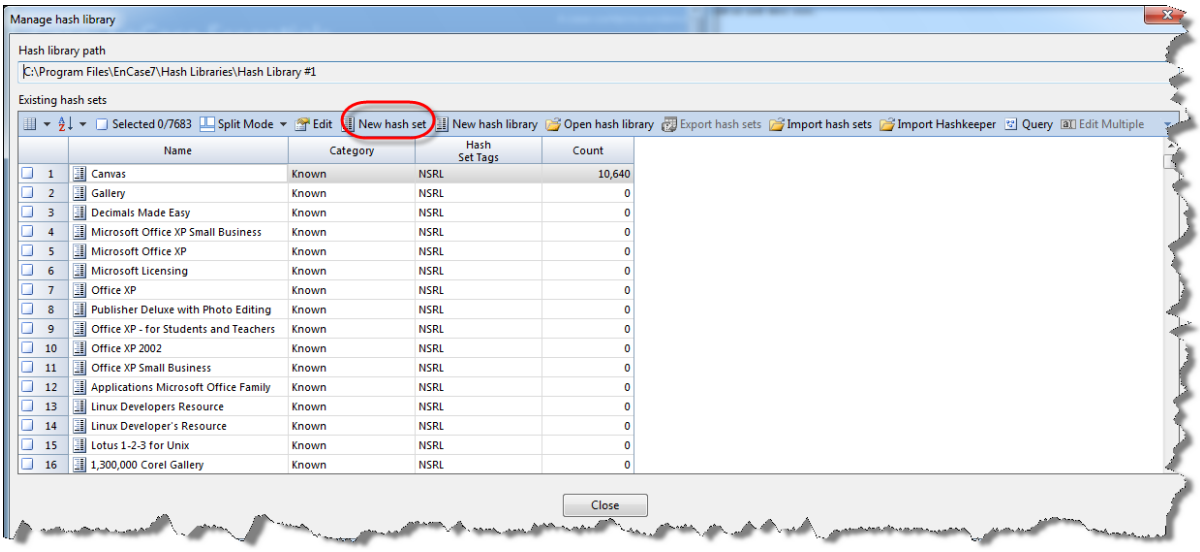

Figure 3-48 New Hash Set

CASE HASH LIBRARY

Your case can have up to two hash libraries. From the case Home screen, click on **Hash Libraries**.

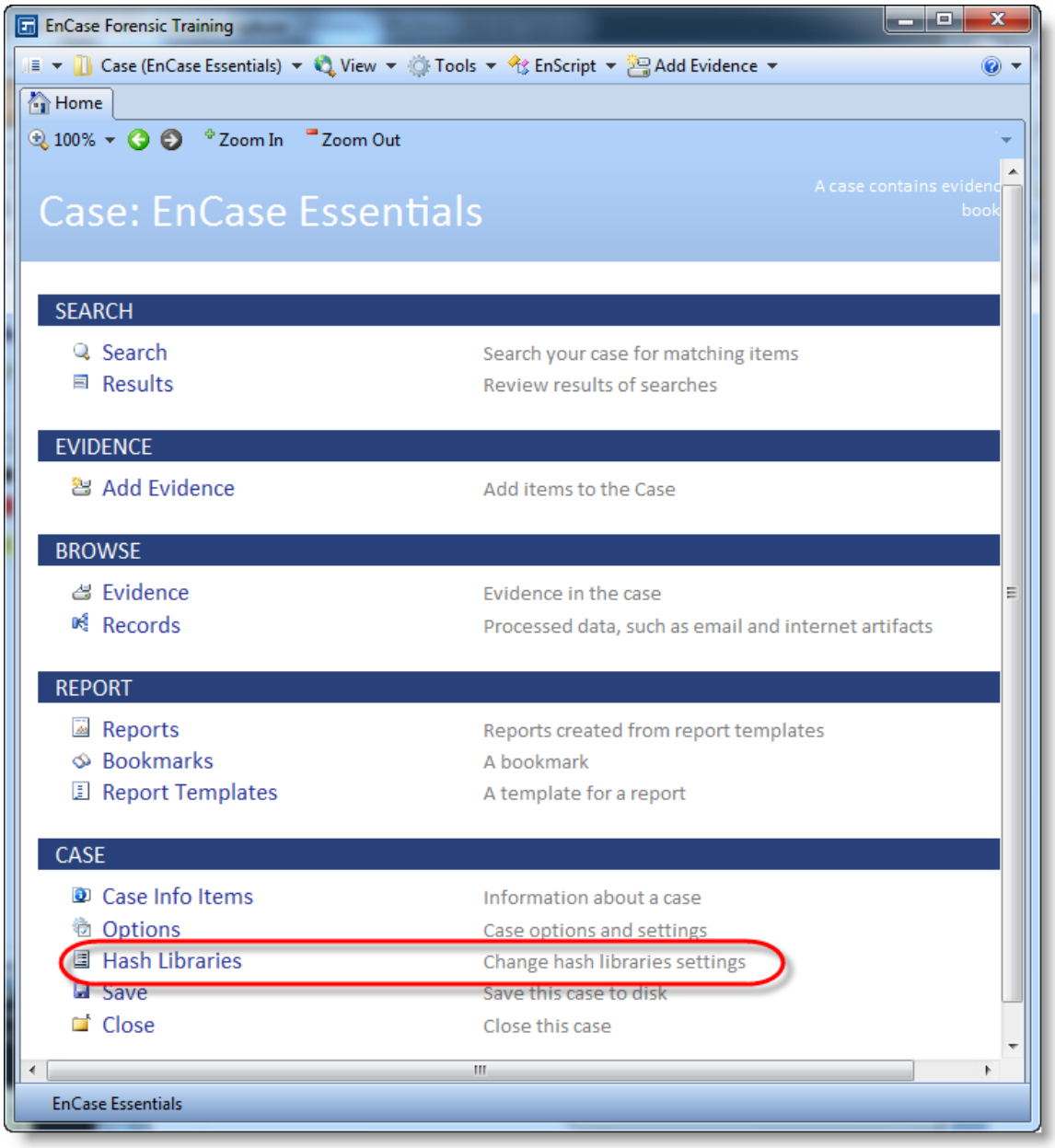

Figure 3-49 Hash Libraries

To select a hash library, click on **Change Hash Library**.

Browse to the Primary hash library and click **OK**.

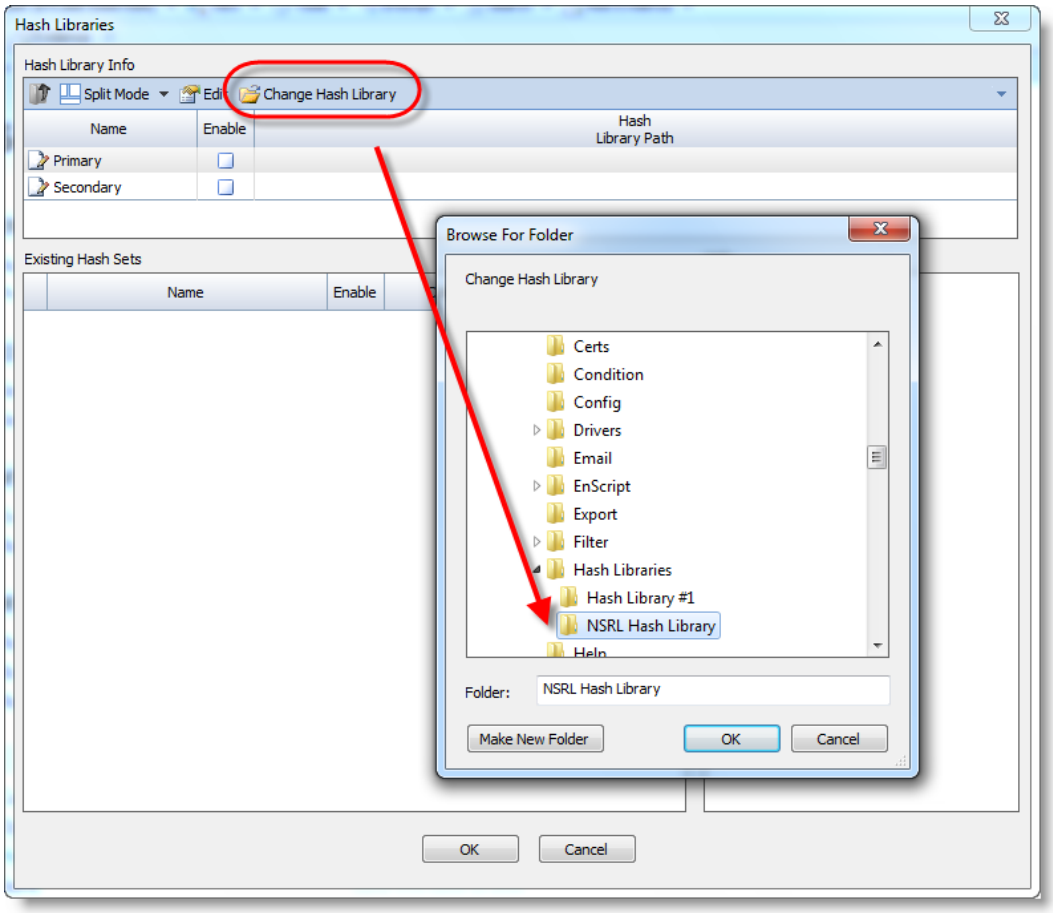

Figure 3-50 Change hash library

The Primary hash library will now be enabled and ready for use with the Evidence Processor. You can also select a Secondary hash library.

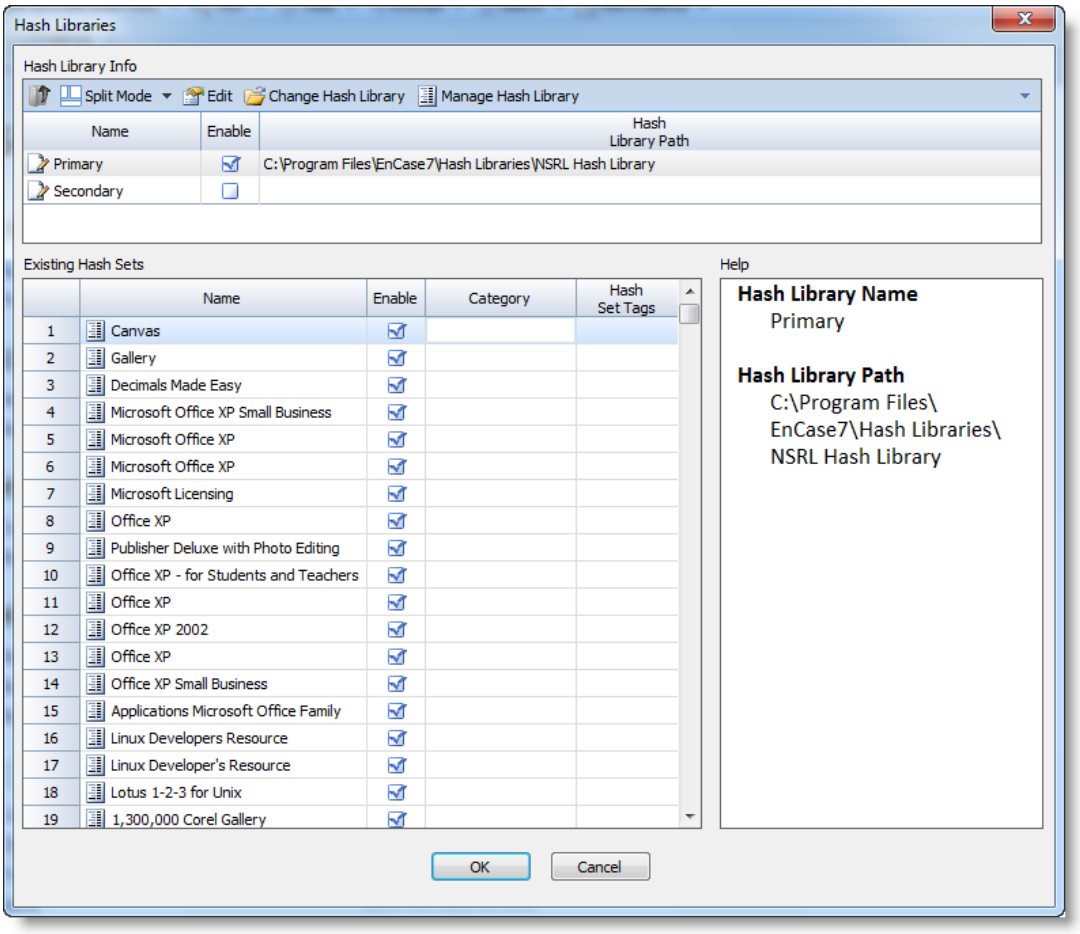

Figure 3-51 Case Hash Libraries

IMPORTING ENCASE LEGACY HASH SETS

EnCase v7 has an EnScript program to import hash sets from prior versions of EnCase.

From the **Tools** menu, select **Import EnCase Legacy Hash Sets...** to run the EnScript module.

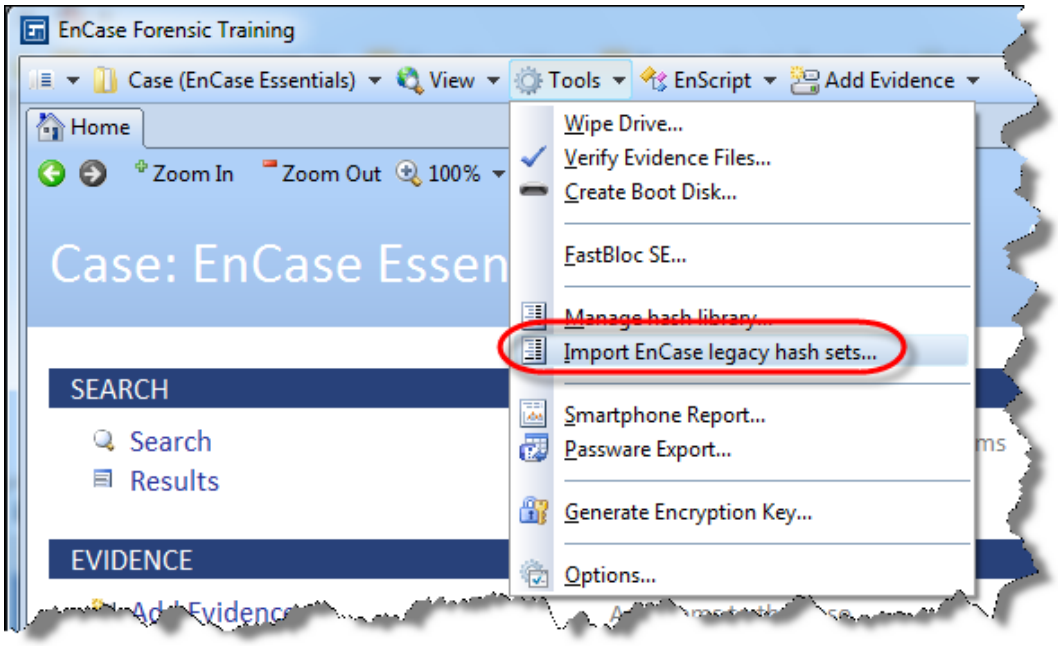

Figure 3-52 Manage Hash Library

Notes

Notes

Notes

Adding Evidence to a Case

New Method to Add Evidence

Add Device in EnCase® v6

In EnCase v6, the Add Devices wizard allowed you to do the following:

- Preview devices (local and enterprise)
- Preview physical and process memory (local and enterprise)
- Preview via a crossover cable
- Add image files (including E01s, L01s, Safeback, vmdk, etc.)
- Preview a Palm device

New Add Evidence Function in EnCase® v7

Again, for instruction on acquiring digital evidence please consider attending one or more of the following courses:

Course	Course website
First Responder with EnCase® Forensic, Tableau, and EnCase® Portable	http://www.guidancesoftware.com/EnCase-First-Responder.htm
EnCase Computer Forensics I	http://www.guidancesoftware.com/computer-forensics-training-encase1.htm
EnCase® Portable Configuration and Examinations	http://www.guidancesoftware.com/encase-portable-examinations.htm

In EnCase v7, functionality that was in EnCase v6 Add Devices wizard is split into separate menus. These menus are accessed from the **Add Evidence** button on the Home page or the drop-down menu.

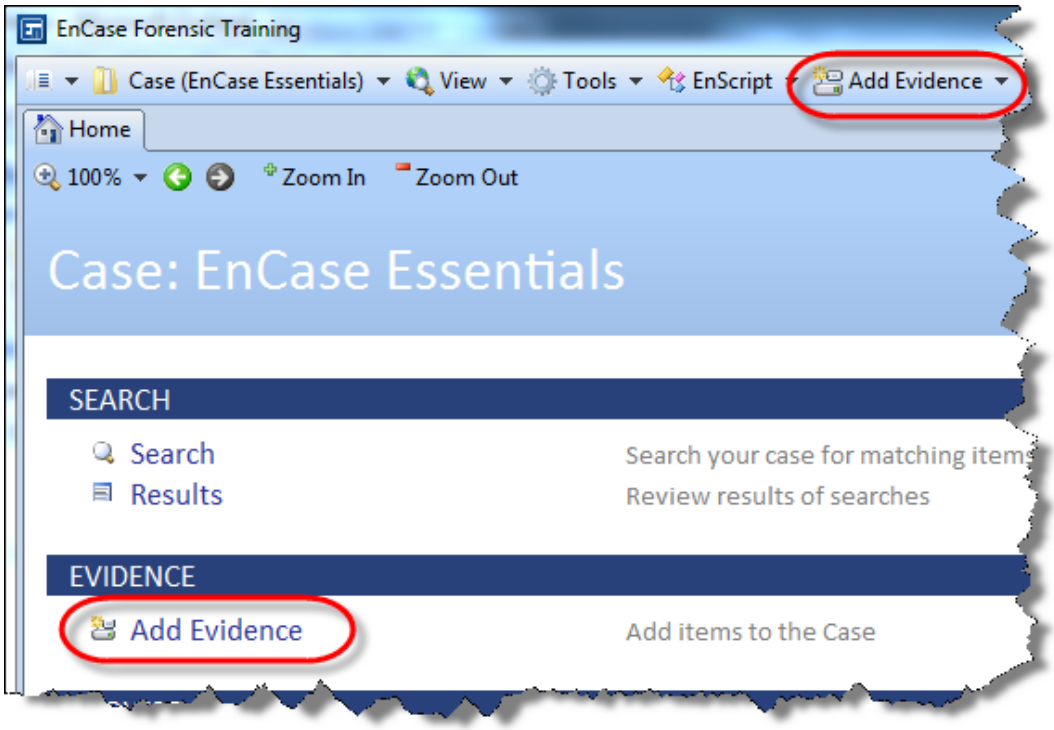

Figure 4-1 Add Evidence

The **Add Evidence** window appears for the Case.

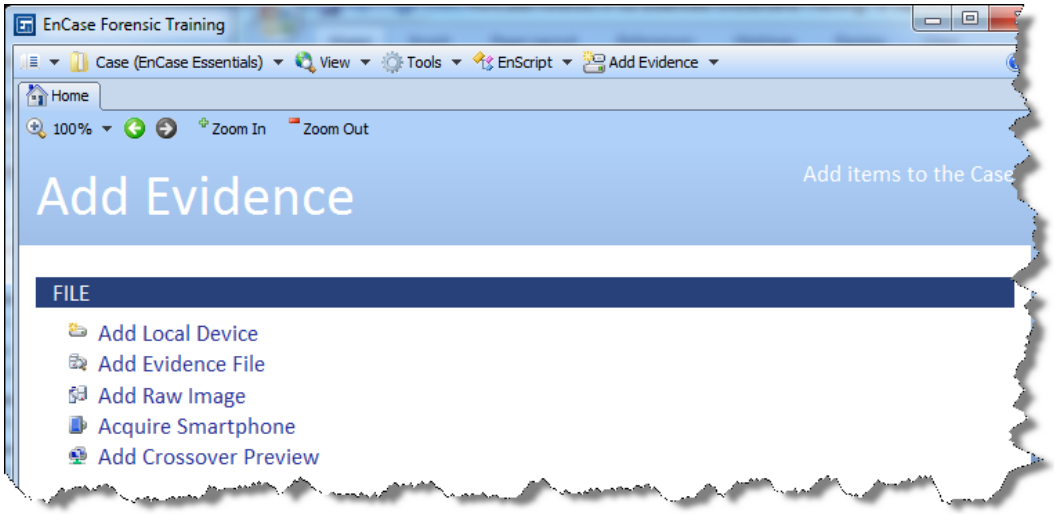

Figure 4-2 Add Evidence

The new menus are:

- **Add Local Device** – Initiate the process of adding a local device attached directly to your local computer. This can be the main system drive, removable drive write blocked with FastBloc SE, or a device attached through a Tableau write blocker.

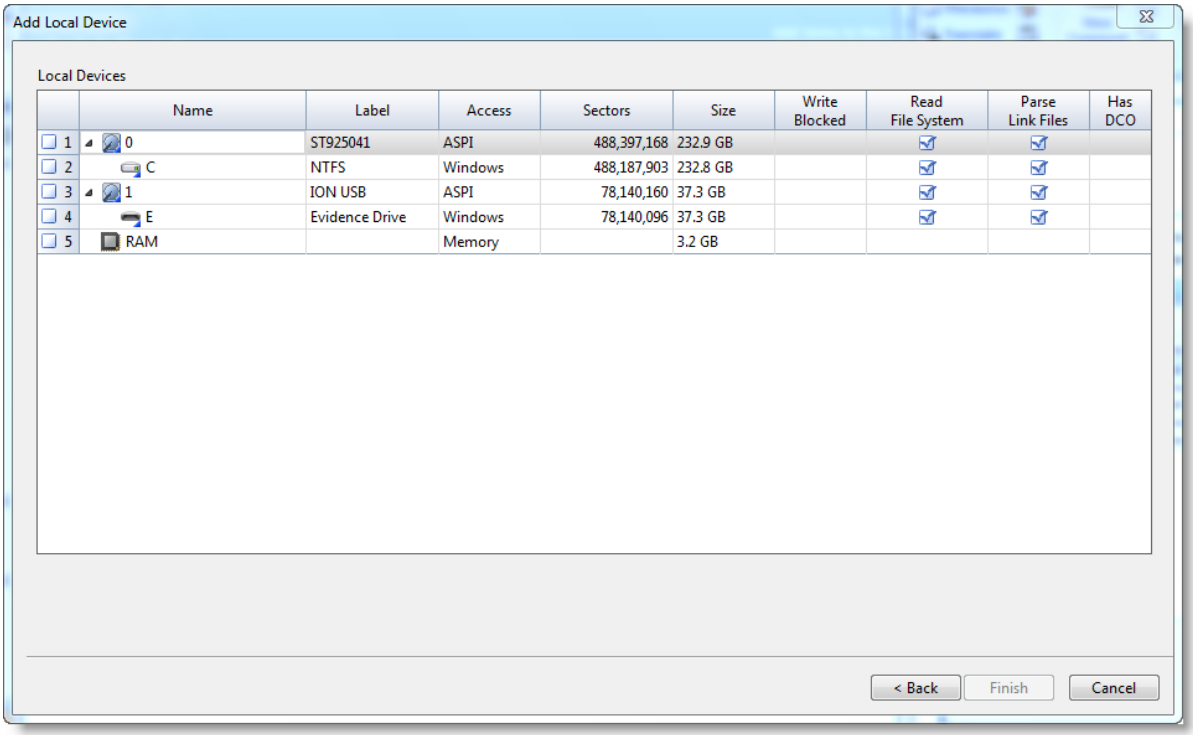

Figure 4-3 New EnCase v7 Add Local Device interface

- **Add Evidence File** – Specify an evidence file to add to the active case. This can be an EnCase evidence file (E01) or logical evidence file (L01).
- **Add Raw Image** – Add a raw or dd image file of a physical device to the active case.

- **Acquire Smartphone** – Acquires a Smartphone. After clicking the **Acquire Smartphone** link, the dialog allows you to specify the device type and the kinds of data that you want to collect into an evidence file.
  - EnCase supports both iOS 5.0 and iOS 5.1 for iPhone and iPad devices. The supported features are the same for all iOS versions, from iOS version 3.0 through 5.1.

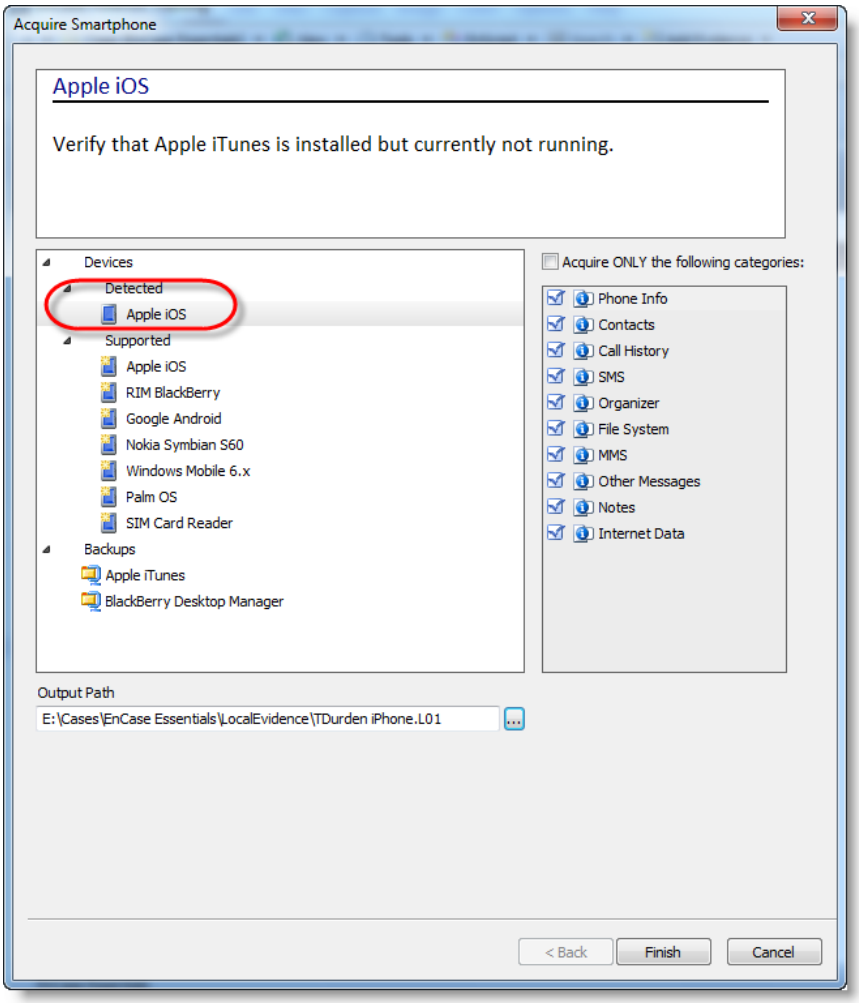

Figure 4-4 New EnCase v7 Smartphone interface

- **Add Crossover Preview** – Crossover-cable acquisitions require both a subject and forensic machine. This type of acquisition also negates the need for a hardware write blocker. It may be desirable in situations where physical access to the subject machine's internal media is difficult or not practical. This is the recommended method for acquiring Macintosh laptops (or others with difficult hard drive removal) and exotic RAID arrays. This option allows you to preview a machine acquired through a crossover-cable acquisition.

  NOTE: Guidance Software is no longer supporting legacy Palm devices.

ADD EVIDENCE FILE

For this course, we will add the TDurden.Ex01 evidence file. There are two methods, select the **Add Evidence** menu or hyperlink.

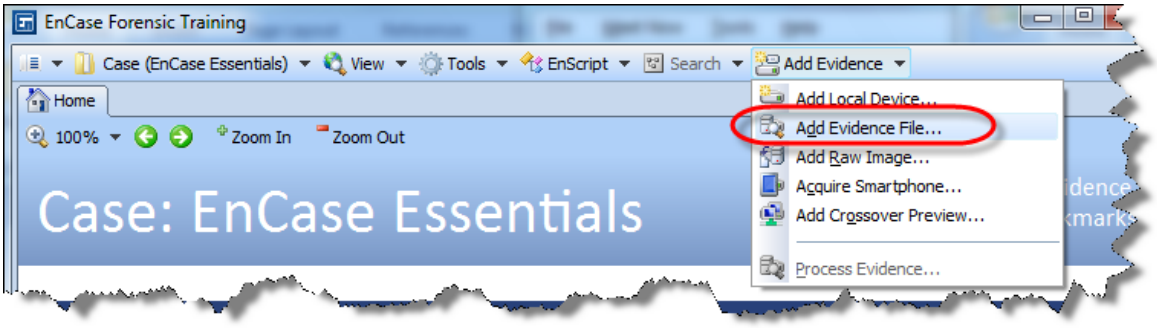

Figure 4-5 Add Evidence hyperlink and menu

Or, if the **Add Evidence** hyperlink was selected, click on **Add Evidence File**.

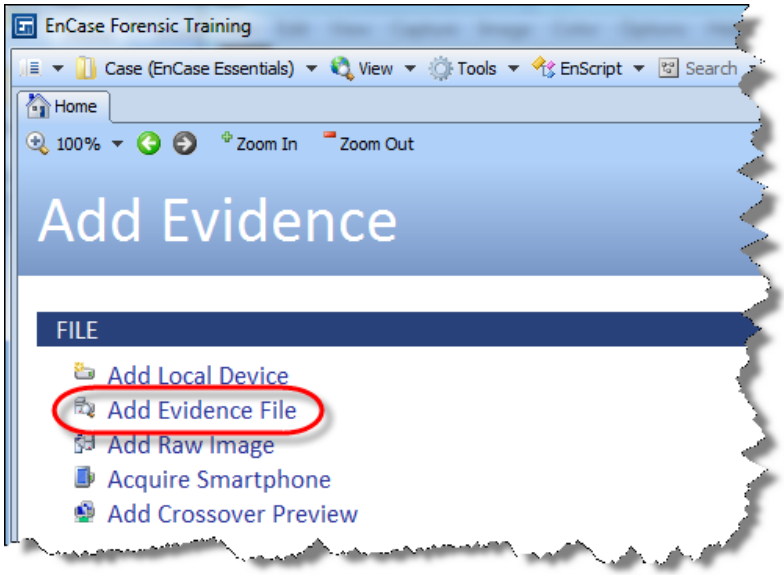

Figure 4-6 Add evidence

Browse to the **TDurden.Ex01** evidence file that you copied to the examination drive and click **Open**.

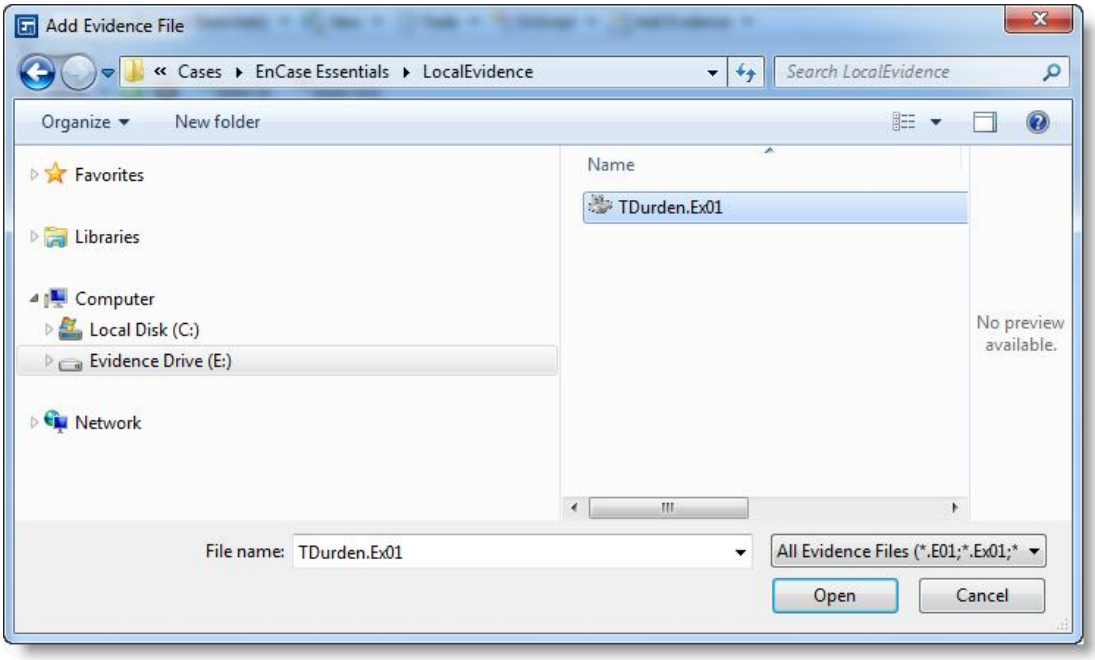

Figure 4-7 Selecting the evidence file

EnCase v7 will then add the device to the case Evidence tab and automatically begin the verification process of the evidence file hash value and CRCs, unless you specifically choose the option to not verify evidence files (***certainly not recommended***).

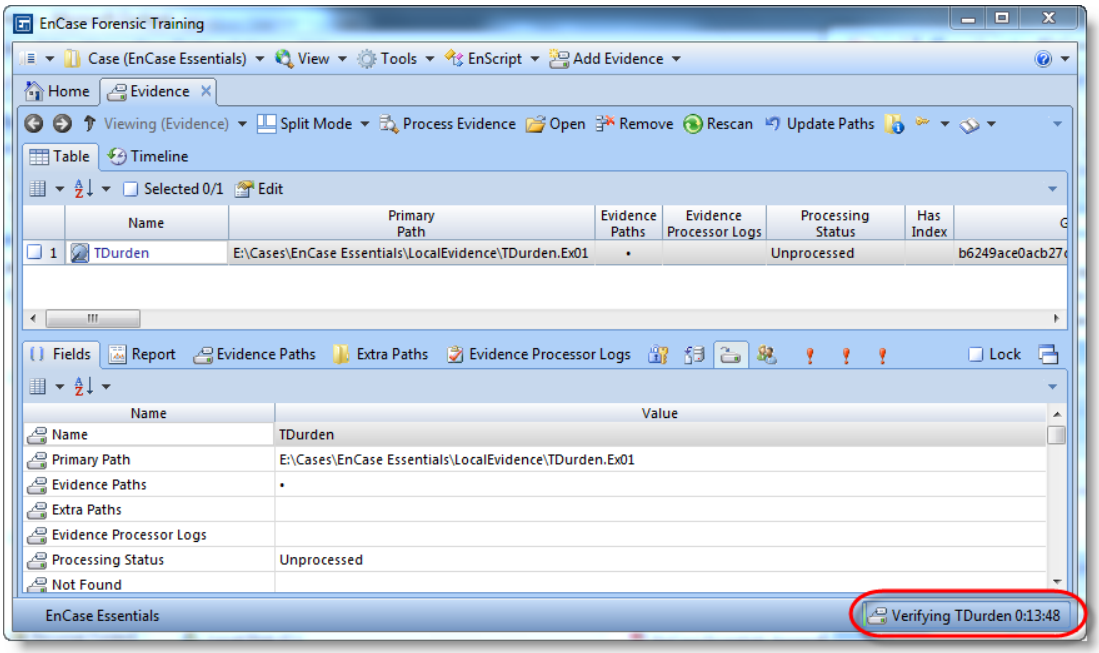

Figure 4-8 Added evidence verifying

When completed, save your case.

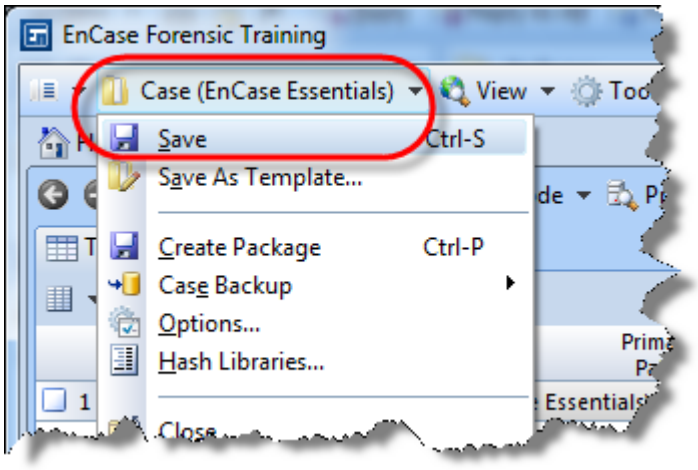

Figure 4-9 Saving your case

EVIDENCE TAB

The Evidence tab allows you to browse selected devices as in previous versions of EnCase® software (EnCase). To browse a single item of evidence, click on the hyperlink in the Name column.

Click on **TDurden**.

EnCase will parse the Master File Table (MFT) and allow you to browse the file structure.

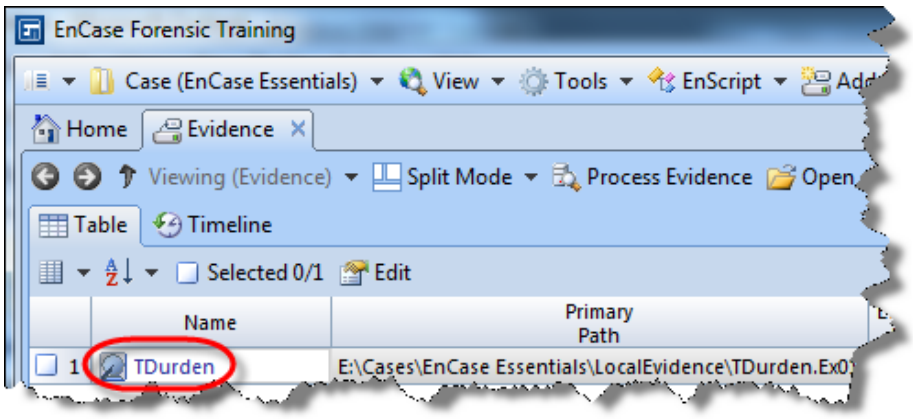

Figure 4-10 Click the hyperlink for the evidence device

If you desire to open two or more devices, blue-check the evidence and click **Open**.

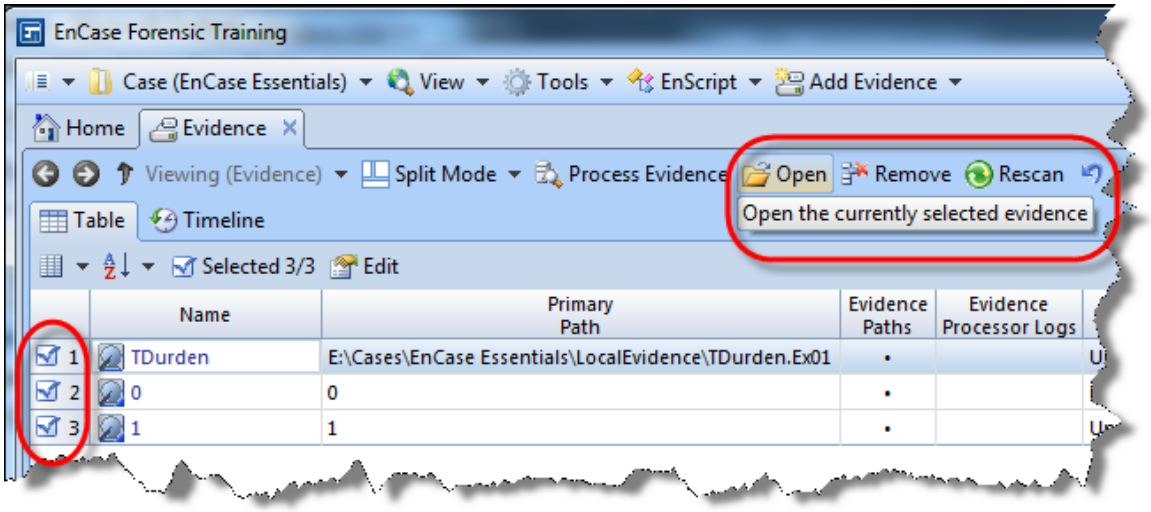

Figure 4-11 Open Selected Evidence

To remove evidence, blue-check the device and click **Remove Selected Evidence**.

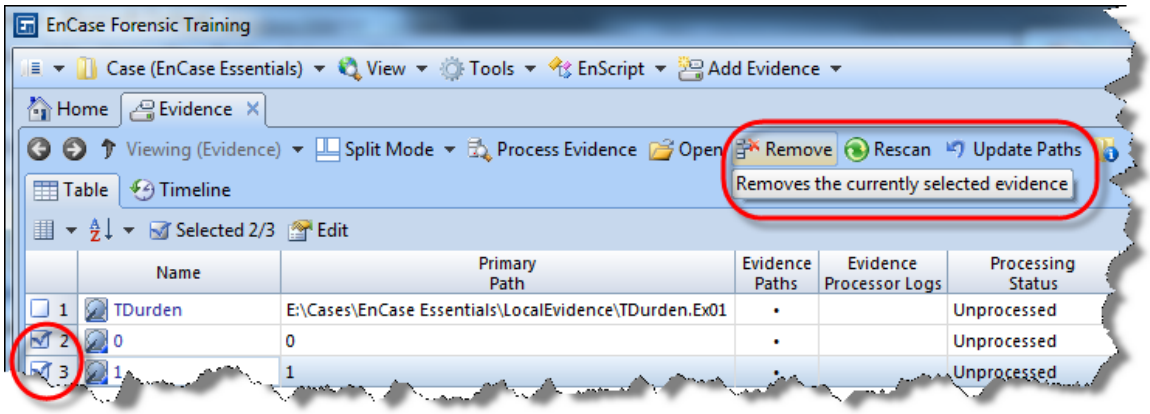

Figure 4-12 Remove Selected Evidence

NAVIGATING THE ENCASE EVIDENCE

When you load evidence, the Evidence tab will open a Tree-Table view for evidence browsing as familiar to EnCase® software users.

The Evidence browsing screen is divided into three sections:

- Tree Pane (left pane)
- Table Pane (right pane)
- View Pane (bottom pane)

The selections in the Tree Pane affect the Table Pane; the selections in the Table Pane affect the View Pane.

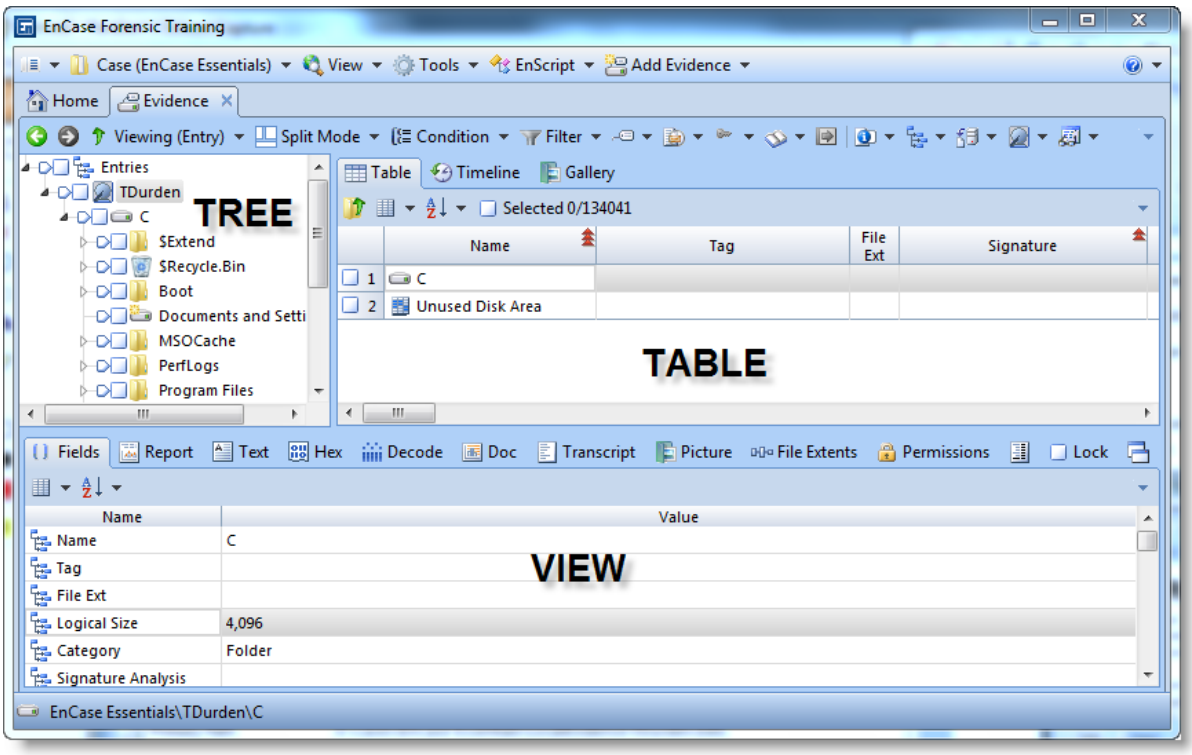

Figure 4-13 Browsing evidence

You can change the split of the screen with the **Split Mode** button and select the preferred-viewing screen based on the investigation you are conducting.

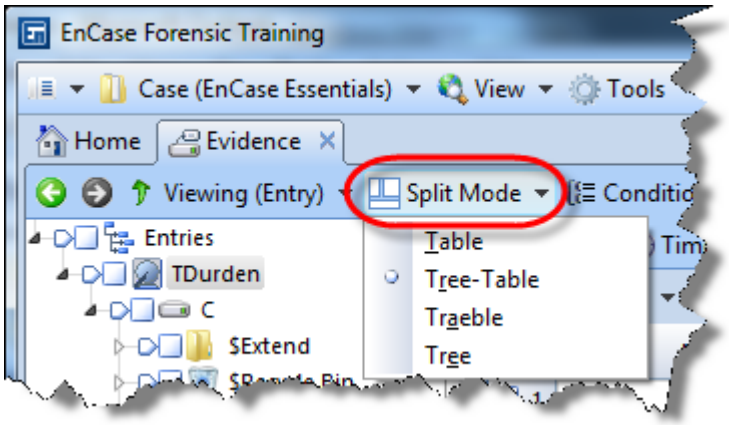

Figure 4-14 Split Mode

- **Table** – Table in top pane and View in bottom pane (no Tree view)
- **Tree-Table** – Default view with Tree in left pane, Table in right pane and, View in bottom pane); this is the traditional EnCase® Entries view
- **Traeble** – Table in top pane and View in bottom pane with the ability browse the folder structure in the Name column
- **Tree** – Tree in left pane and View in right pane (no Table view)

Tree Pane / Evidence View

Within the Tree view you have a tree-structured view of the evidence. It presents each evidence file as a folder that contains additional folders. Only evidence files and the folders contained within them are displayed in this view. Individual files are displayed in the Table Pane (discussed later). The arrows can be used to expand and contract the tree structure just as they are used in Windows® Explorer.

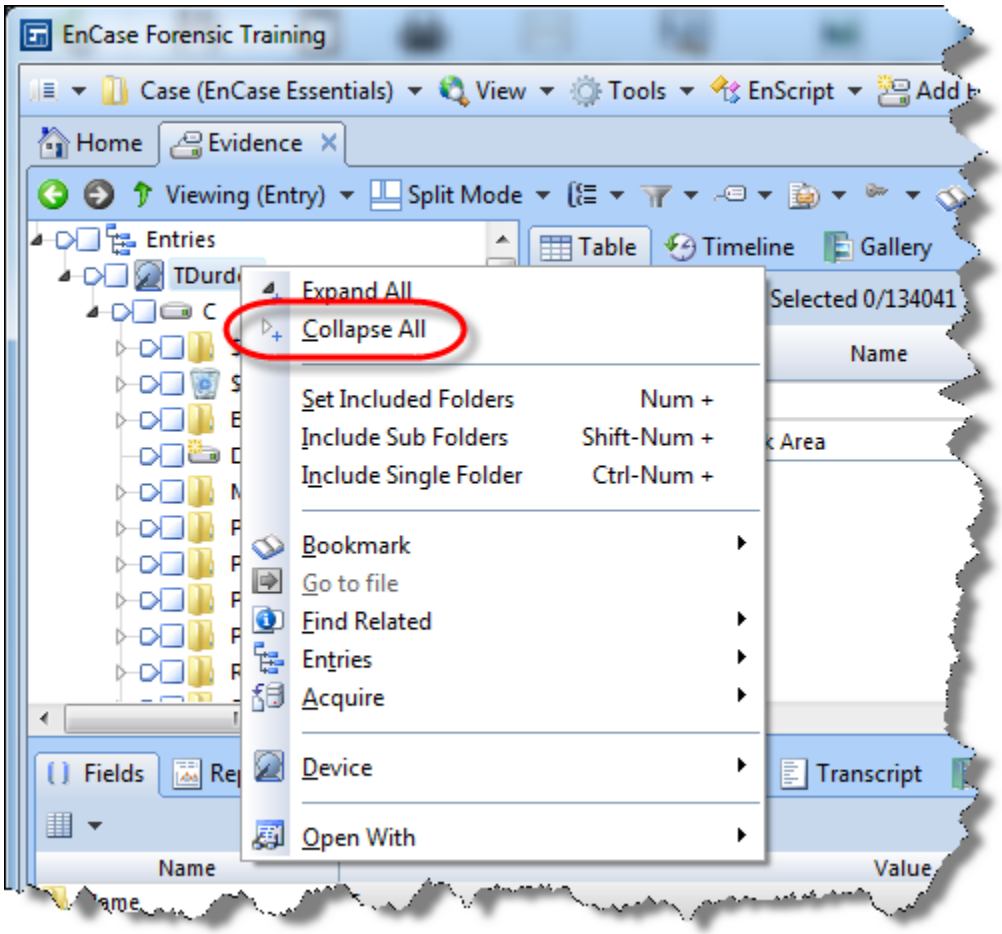

Figure 4-15 Collapsing a folder structure

There are three methods used within EnCase v7 to focus on specific files or folders. These methods have different purposes:

- Highlighting a folder displays the entries within that folder in the Table Pane (this is used for viewing information only).

- The **Set Included Folders** option method (sometimes called the "polygon" or "home plate") displays all the entries, files, and folders for that folder and all subfolders in the Table Pane. It overrides the highlighting option. It is activated by clicking on the polygon next to the tree of the folder name in the Tree Pane in the Evidence→Viewing (Entry) view and in any other views displaying a similar folder structure. This is used for viewing information only. When a folder is *included*, the other folders are *grayed out*. All files and folders within the folder and subfolders are displayed in the Table Pane. To deactivate this function, click on the **Set Include Option** icon again or click twice on another include icon.

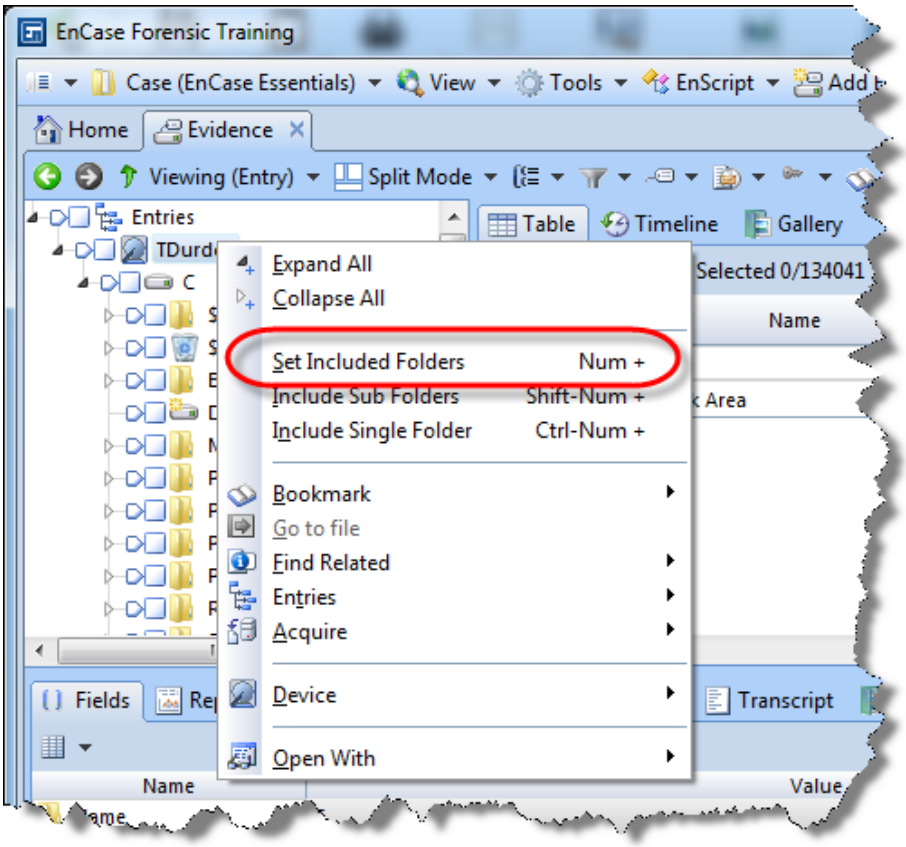

Figure 4-16 "Set including" a folder structure

- The **blue-check** or **Select for future action** method is used for designating files or folders on which to perform an analysis operation, such as a keyword search. This can be implemented from a variety of views. It is activated by clicking on the square next to the tree of the entry name in any view.

In the following example, several folders have been selected. These folders have a white background within the *blue-checked* square (☑) indicating that all entries within the folder have been selected. If there is a gray background within the blue-checked square (☑), it indicates not all entries within the folder have been selected. The **Selected** box above the Table Panes indicates how many entries have been selected. To deselect all entries, click within this **Selected** box to remove the blue-check and to remove blue-checks from elements of the Evidence→Viewing(Entry) view and the Table Pane.

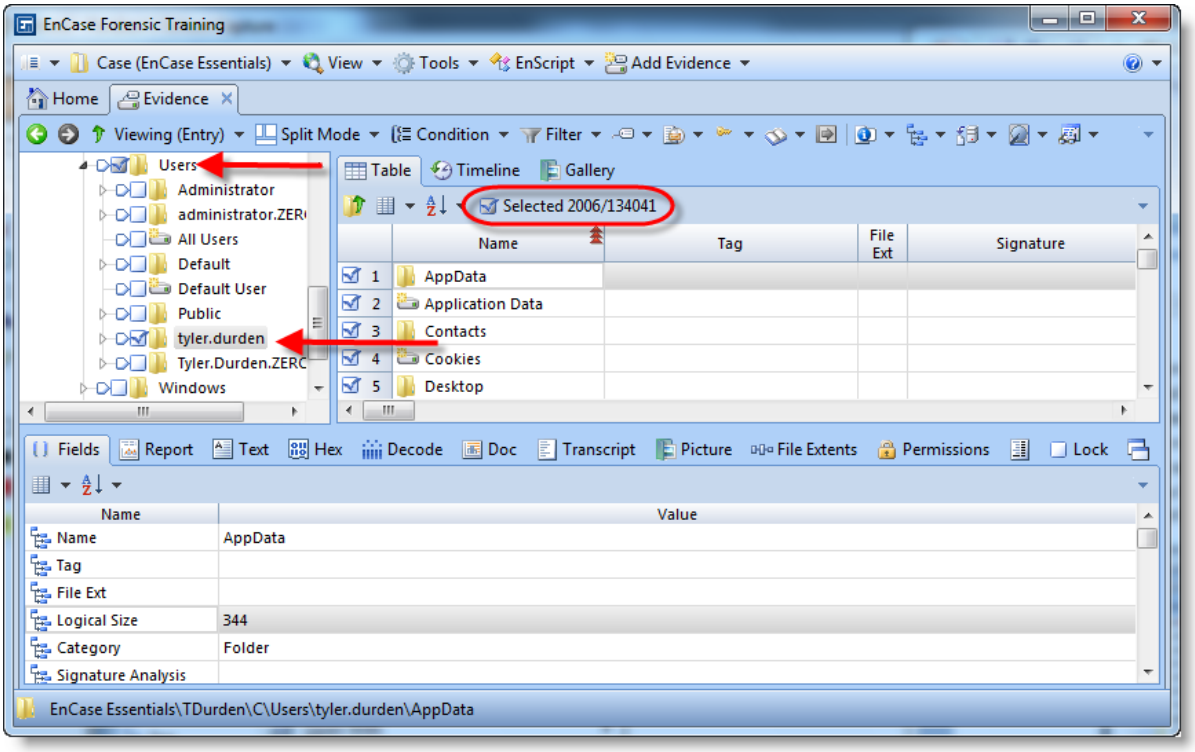

Figure 4-17 Blue-checking entries and the Selected box

RIGHT-CLICK

Veteran users of previous versions of EnCase are trained to right-click on an object in the Tree Pane to bring up a context menu with many selection options. Also, there is a drop-down menu on the far right side of the menu bar.

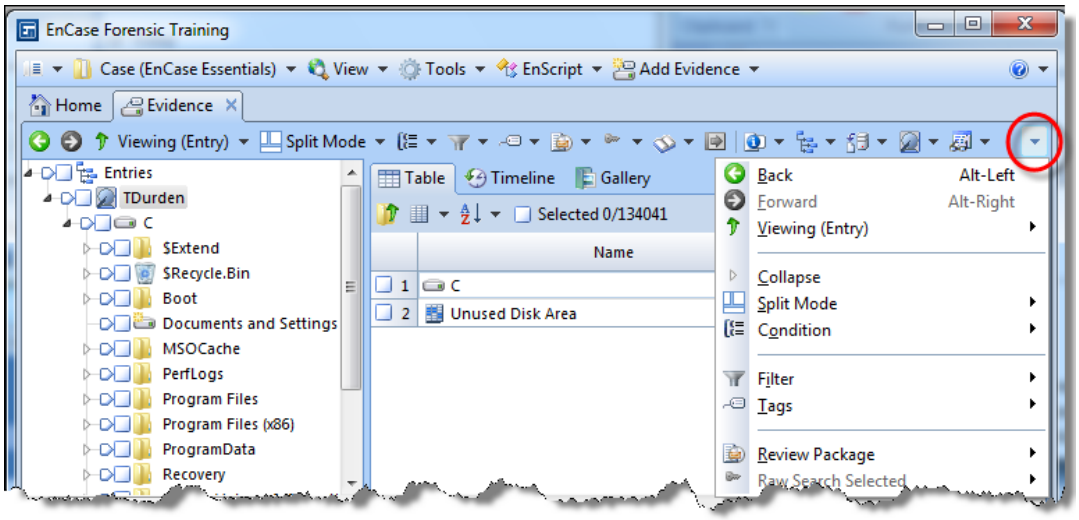

Figure 4-18 The new drop-down menu in EnCase v7

ADDITIONAL VIEWS

Within the Tree Pane there are many views that can be accessed for different purposes. All of these views may be accessed through the tabs available above the Tree Pane or through the View menu. Any tabs not displayed above the Tree Pane will be displayed by selection through the View menu.

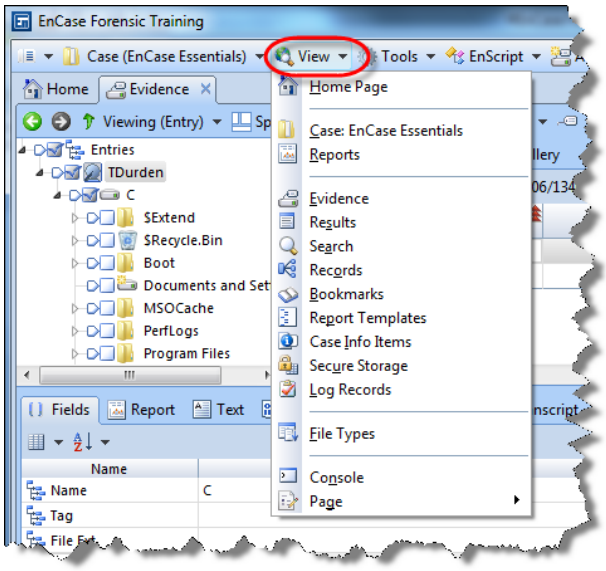

Figure 4-19 View→Cases menu

Table Pane

By default the Table Pane is in the Table view. Within this view are the subfolders and files that are contained within the folder(s) and highlighted or included (Set Included Folders) in the Tree Pane. Highlighting or including (Set Included Folders) a folder affects the display in the Table Pane as previously explained.

The *highlighting* and Set Included Folders features are intended to view desired files and folders in the Table Pane. If there are one or more folders designated with the *include* feature, the highlighting feature will not change the number of files/folders displayed in the Table Pane.

This differs from the Selected box located to the right of the pointed box. This is intended to select with a blue-check the files and folders on which to perform certain operations, including but not limited to searching, copying, and exporting. With the Set Included Folders feature activated, the select operation will not alter the number of files/folders displayed in the Table Pane.

The Table view in the Table Pane displays many columns of information about the displayed entries:

- **Name** identifies the file/folder/volume, etc., in the evidence file.
- **Tag** displays the tag(s) placed by you on an entry.
- **File Ext** displays the entry's extension, which initially determines whether this entry is displayed in the Gallery view.
- **Logical Size** specifies the file size as the operating system addresses the file.
- **Item Type** identifies the type of evidence, such as Entry (file or folder), Email, Record, or Document.
- **Category** indicates the category of the file from the File Type table.
- **File Type** (formerly Signature) displays signature of a Match or an Alias (renamed extension).
- **Signature Analysis** the results of a file signature analysis.
- **File Types Tag** displays the Unique Tag (from the File Types table) for the entry after a file signature analysis (this column can be activated from the Show Columns drop-down menu) This column was formerly called the "Signature Tag."
- **Last Accessed** displays the last accessed date/time. This typically reflects the last time the operating system or any compliant application touched the file (such as viewing, dragging, or right-clicking). Entries on FAT volumes do not have a last-accessed time.
- **File Created** typically reflects the date/time the file/folder was created at that location. A notable exception to this is the extraction of files/folders from a ZIP archive. Those objects will carry the created date/time as they existed when the objects were placed in the archive.
- **Last Written** reflects the date/time the file was last opened, edited, and then saved. This corresponds to the Modified time in Windows with which users are familiar.

- **Is Picture** displays true if the file is an image.

  NOTE: The display depends on how the Show True/False options were set in the Tools→Options→Global menu.

- **Code Page** displays the character encoding table upon which the file is based.
- **MD5** displays a 128-bit value for a file entry generated by a hash analysis process.
- **SHA1** displays the SHA-1 hash value for a file entry generated by a hash analysis process.
- **Item Path** identifies the location of the file within the evidence file, including the evidence file name and a volume identifier.
- **Description** describes the *condition* of the entry – whether it is a file or folder, deleted, or deleted/overwritten.
- **Protected** indicates if the file is identified as an encrypted or password-protected file during the Evidence Processing.
- **Protection complexity** provides details on the file's protection.
- **Is Deleted** displays *True* if the entry is in a deleted state; blank if it is not.
- **Entry Modified** indicates when the administrative data for the file was last altered for NTFS and Linux.
- **File Deleted** displays the deleted date/time if the file is documented in the Recycle Bin's Info2 file.
- **File Acquired** identifies the date/time the evidence file in which this entry resides was acquired.
- **Initialized Size** indicates the size of the file when it is opened; applies only to NTFS file systems.
- **Physical Size** specifies the size of the storage areas allocated to the file.
- **Starting Extent** identifies the starting cluster of the entry.
- **File Extents** displays the cluster fragments allocated to the file. Click within this column for an entry and then click on the **Details** tab in the View Pane to see the cluster fragments.
- **Permissions** shows security settings of a file or folder in the View Pane.
- **Physical Location** displays the number of bytes into the device at which the data for an entry begins.
- **Physical Sector** lists the sector number into the device at which the data for an entry begins.
- **Evidence File** displays where the entry resides.
- **File Identifier** displays an index number for a Master File Table (NTFS) or an Inode Table (Linux/UNIX).
- **GUID** indicates the Global Unique Identifier for the entry; to enable tracking throughout the examination process.

- **Hash Sets** displays if a file belongs to one or more hashsets, generated by including hash sets in a hash library in a hash analysis process.
- **Short Name** displays the name Windows gives the entry, using the DOS 8.3 naming convention.
- **VFS Name** is used to display the name for files mounted with the EnCase® Virtual File System (VFS) module in Windows Explorer. This replaces the Unique Name column in previous versions of EnCase.
- **Original Path** displays information derived from data in the Recycle Bin. For files within the Recycle Bin, this column shows where they originated when they were deleted. For deleted/overwritten files, this column shows the file that has overwritten the original.
- **Symbolic Link** displays data pertaining to the equivalent of a Windows Shortcut in Linux and UNIX.
- **Is Duplicate** displays *True* (Yes) if the displayed file is a duplicate of another.
- **Is Internal** indicates whether the file is an internal system file, such as the $MFT on an NTFS volume.
- **Is Overwritten** indicates if the first or more clusters of an entry has been overwritten by a subsequent object.

You can use the Show Columns drop-down menu on dialog box to hide or show columns from your Table Pane.

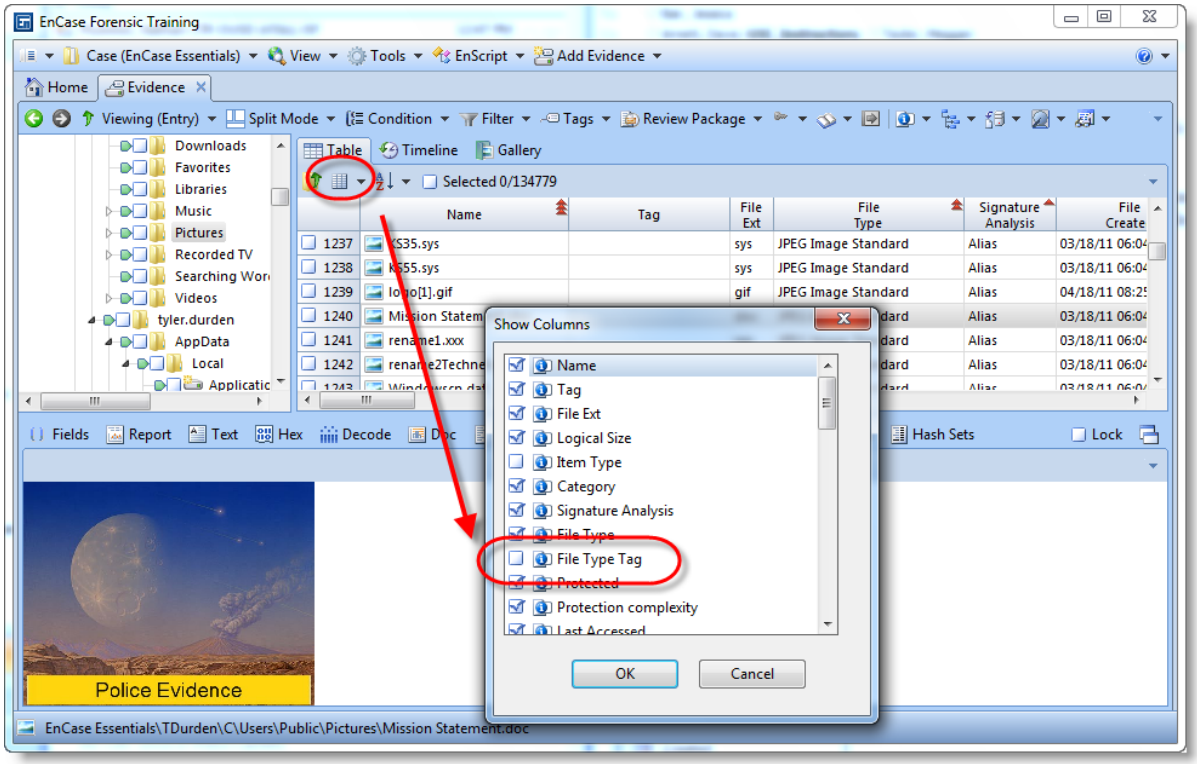

Figure 4-20 Show Columns

Organizing Columns

Table columns may be rearranged in any order just as is done in Microsoft® Excel. Click and hold down on the column heading then drag and drop it into its new location.

Columns may be sorted by up to five layers deep. To sort by a particular column, double-click on the column heading. To institute a sub-sort, hold down the **Shift** key and double-click on the column heading.

Columns may be *locked* on the left side of the Table view so that when you scroll to the right of the Table view, the initial columns are still visible. To lock a column, right-click on the column heading, select **Columns**, and select **Set Lock**. The lock is instituted on the position of the column. If other columns are moved into that position, they are locked. To release the lock, right-click on the column, select **Columns**, and then **Unlock**.

Other Table Pane Views

Gallery

The Gallery view displays images in a thumbnail view. These images are displayed (by default) based on their extension. The Signature Analysis function enables files to be analyzed to see if they were renamed to disguise their existence on the media. To reduce the increase of the number of images displayed at any one file, right-click in the **Gallery** and select **Fewer/More Columns/Rows**.

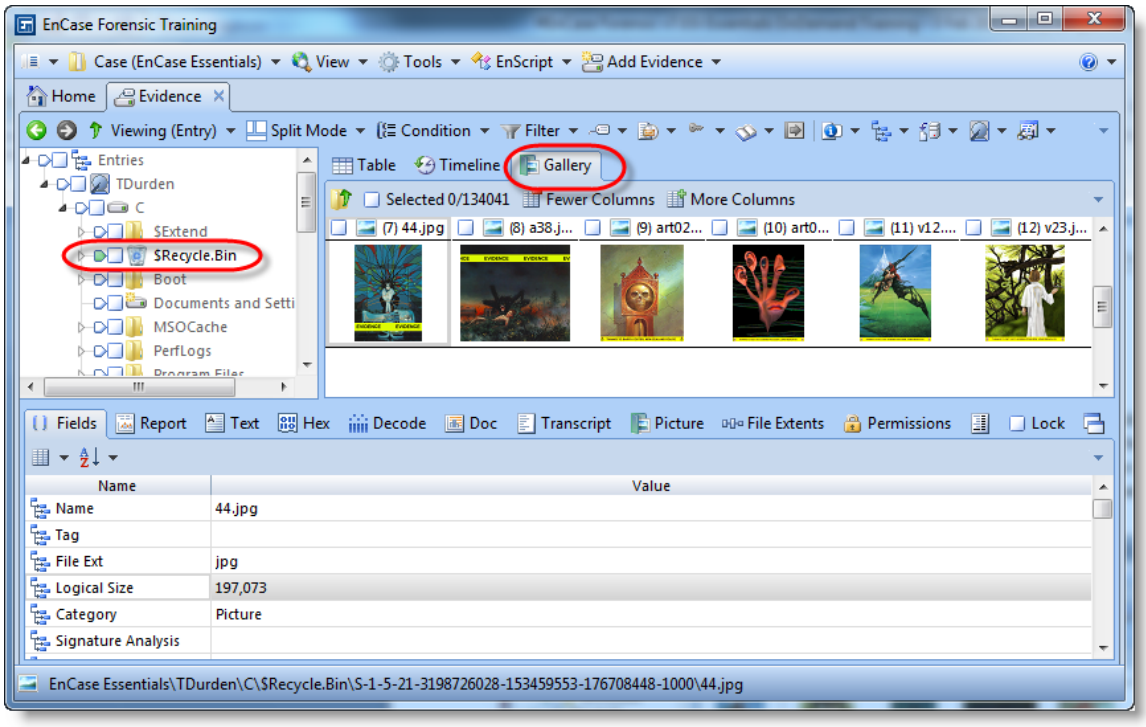

Figure 4-21 Gallery view

BOOKMARKING IN EVIDENCE VIEW

While browsing or following a lead in the Evidence view, should you find evidence you wish to bookmark for inclusion in your final report, blue-check the entry (entries).

Use the Bookmark menu to select **Single item...** (**Ctrl-B**) or **Selected items...** (**Ctrl-Shift-B**) as appropriate.

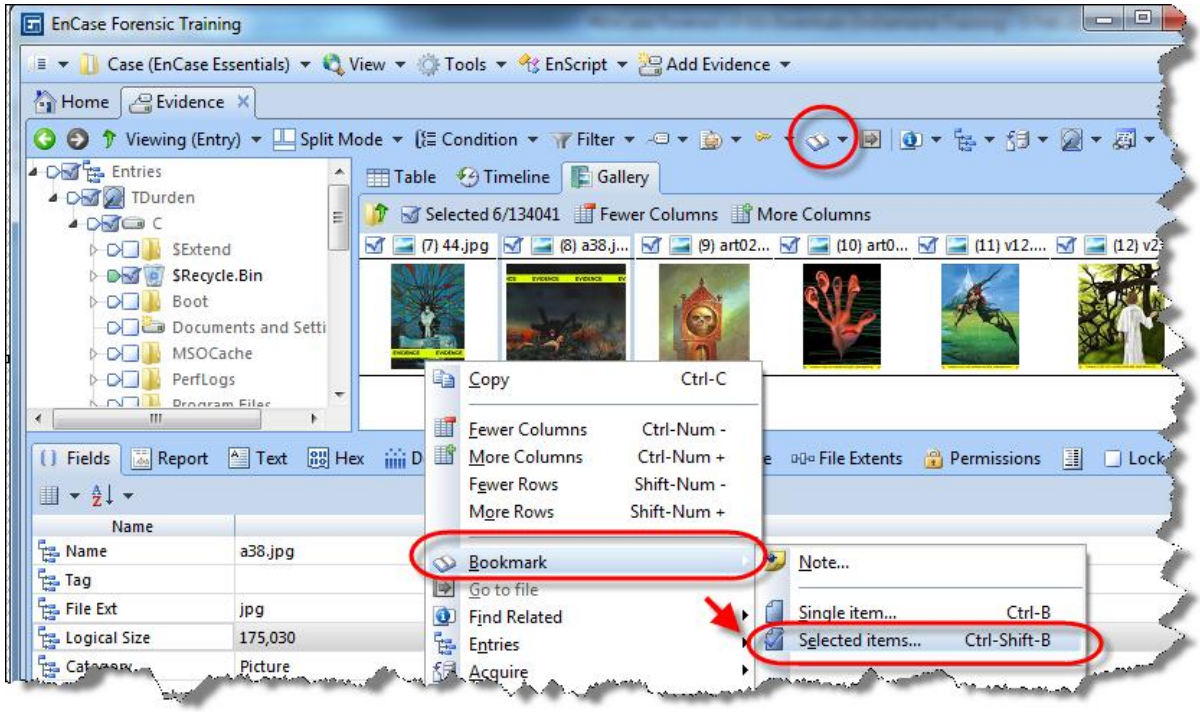

Figure 4-22 Bookmarking selected items

Place the evidence bookmarks in the appropriate folder of your case report template or you can create a new folder.

NOTE: If you bookmark several files (**Ctrl**+**Shift**+**B**), you are not able to add a Bookmark comment. If wish to add a comment to an individual file, then bookmark that **Single File** (**Ctrl**+**B**).

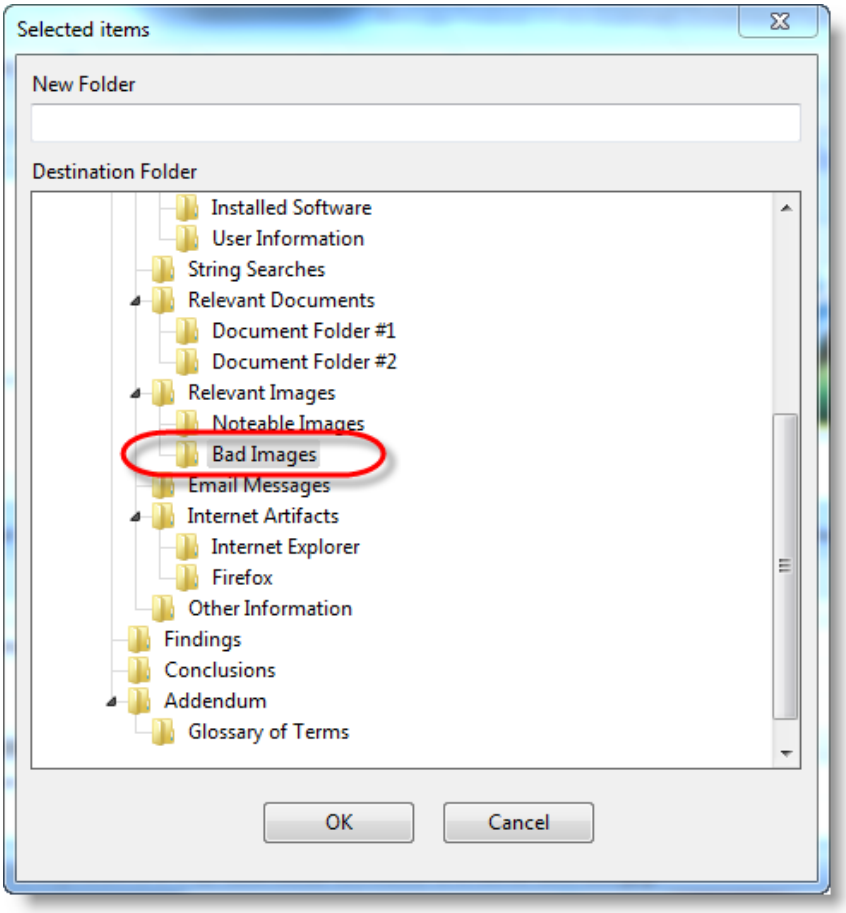

Figure 4-23 Bookmarking selected images

Timeline View

The Timeline view shows patterns of different types of dates and times. You can zoom in (higher resolution) to a second-by-second timeline and zoom out (lower resolution) to a year-by-year timeline.

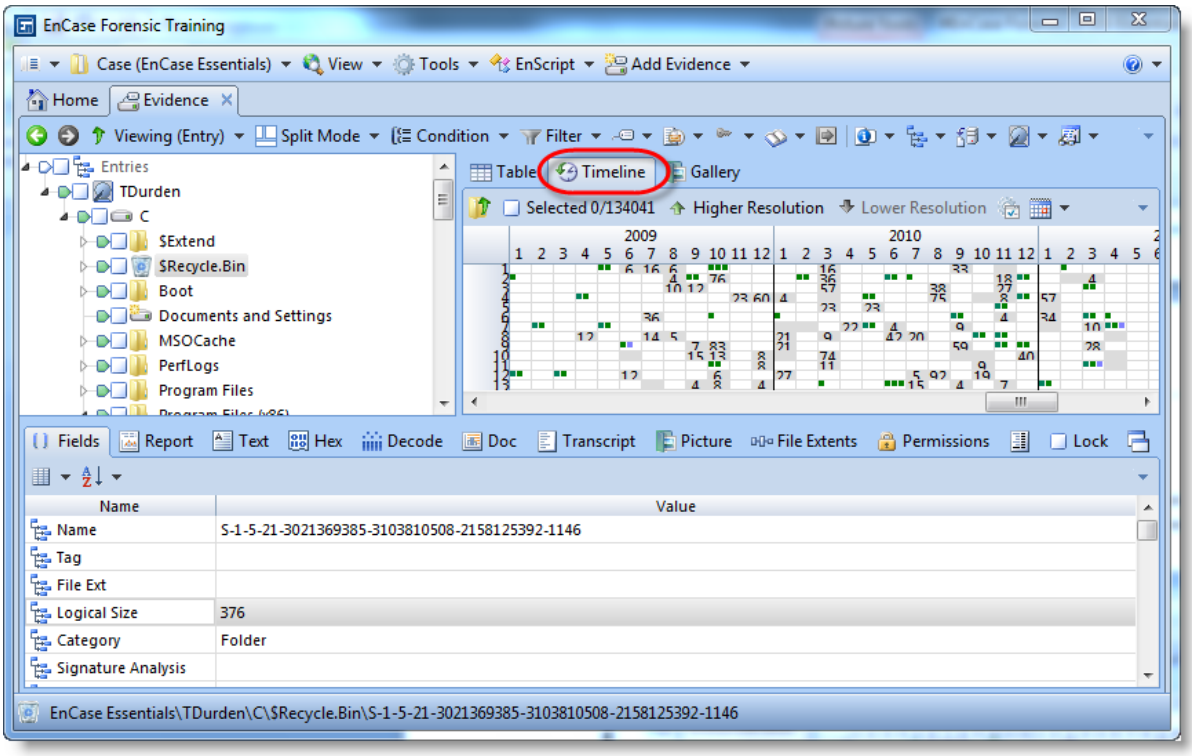

Figure 4-24 Timeline view

Disk View

The Disk view allows viewing of files and folders in terms of where the data appeared on the media. Placement of clusters and/or sectors and fragmentation of files may be observed.

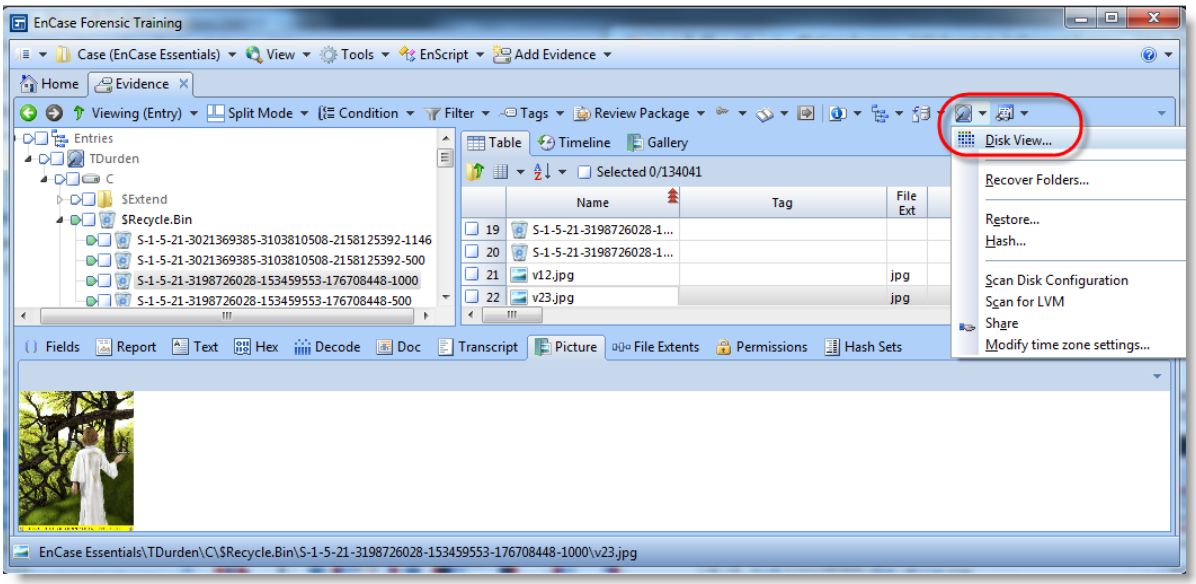

Figure 4-25 Select "Disk View..."

EnCase v7 has a new Auto Extents option in Disk view. When you select a sector, it auto-highlights all of the extents that make up the file. This is different behavior from EnCase v6 (you had to double-click on the sector), and currently you can turn it off with the checkbox.

Click on the **Evidence** tab to return to the entries browsing.

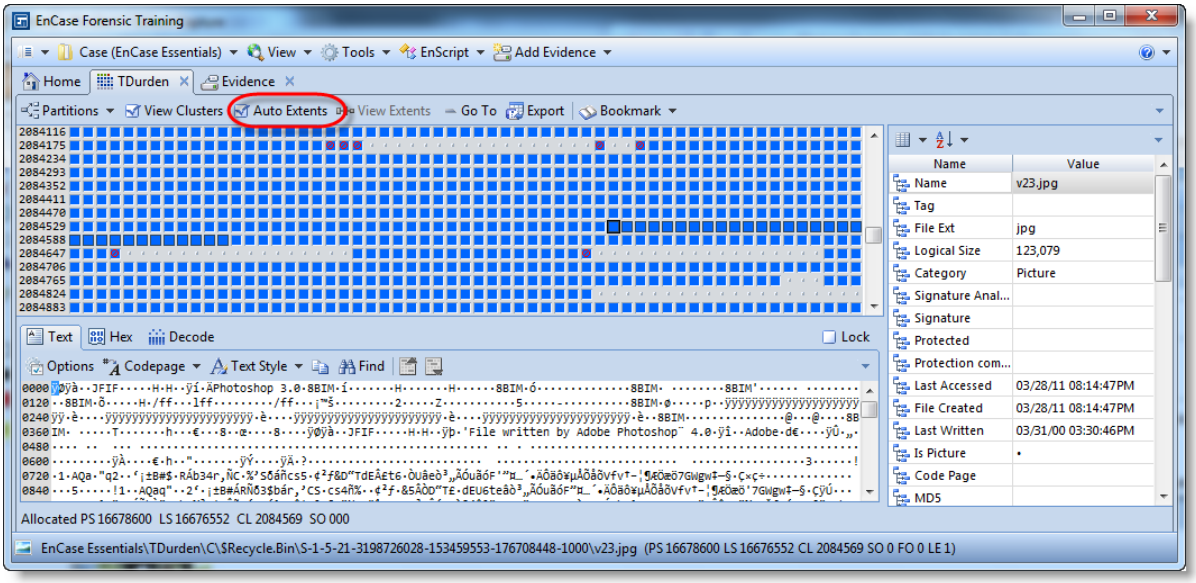

Figure 4-26 Auto Extents – Disk View

VIEW PANE

The View Pane displays the contents of the item highlighted in the Table Pane. The View Pane has default settings that should be understood. Initially the View Pane defaults to the Fields view.

You can undock the View Pane for dual monitors.

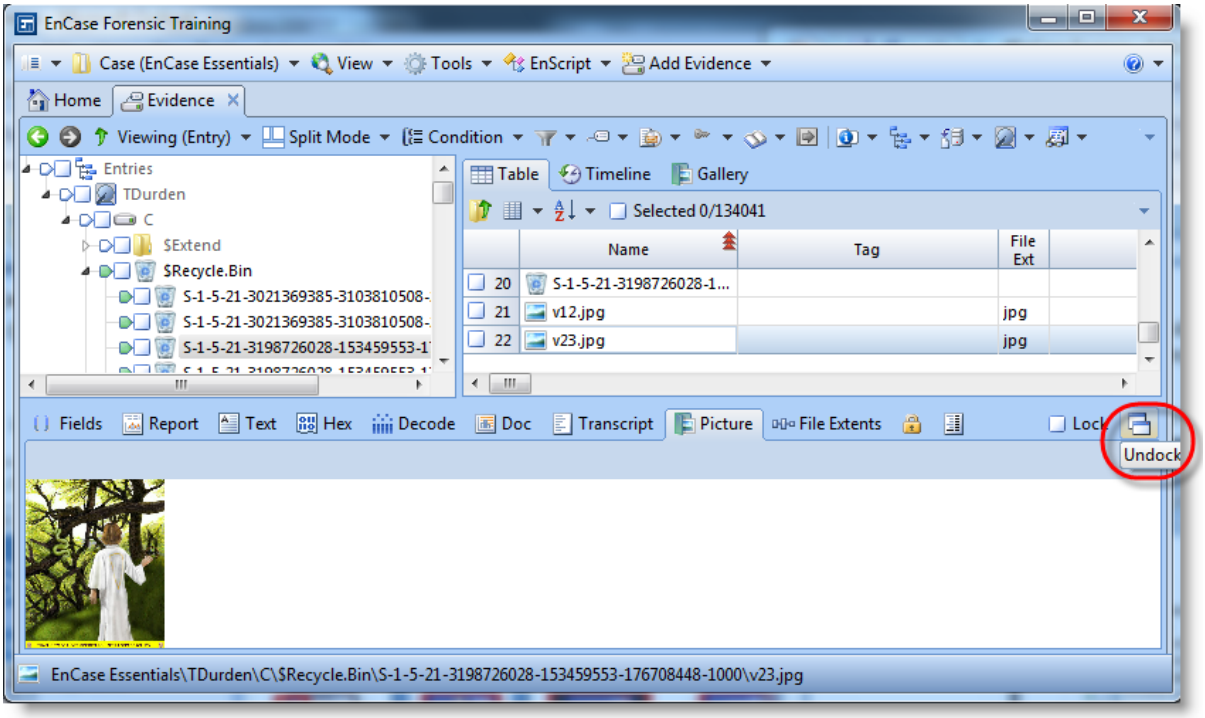

Figure 4-27 Undock the View Pane

To return the View Pane to the main EnCase v7 interface, close the View Pane.

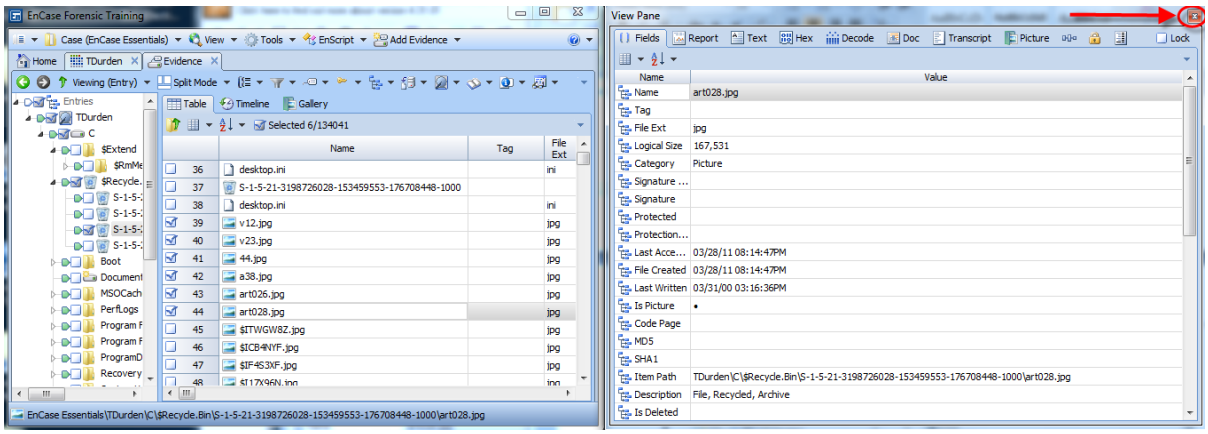

Figure 4-28 Close the undocked View Pane

Fields

The Fields tab provides you with a table of the metadata (data about the file) for the entry. In EnCase v7, all of the fields are able to be searched in an Index query.

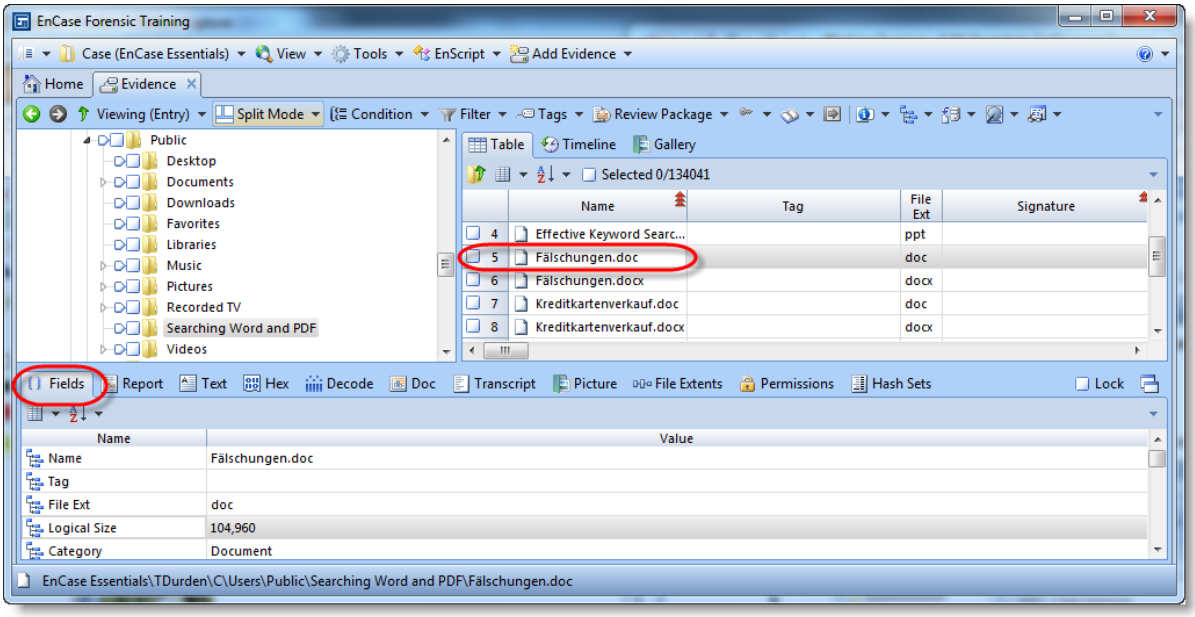

Figure 4-29 DOCX file in the View Pane – Fields tab

Text

The following screenshot displays a document file in Text view.

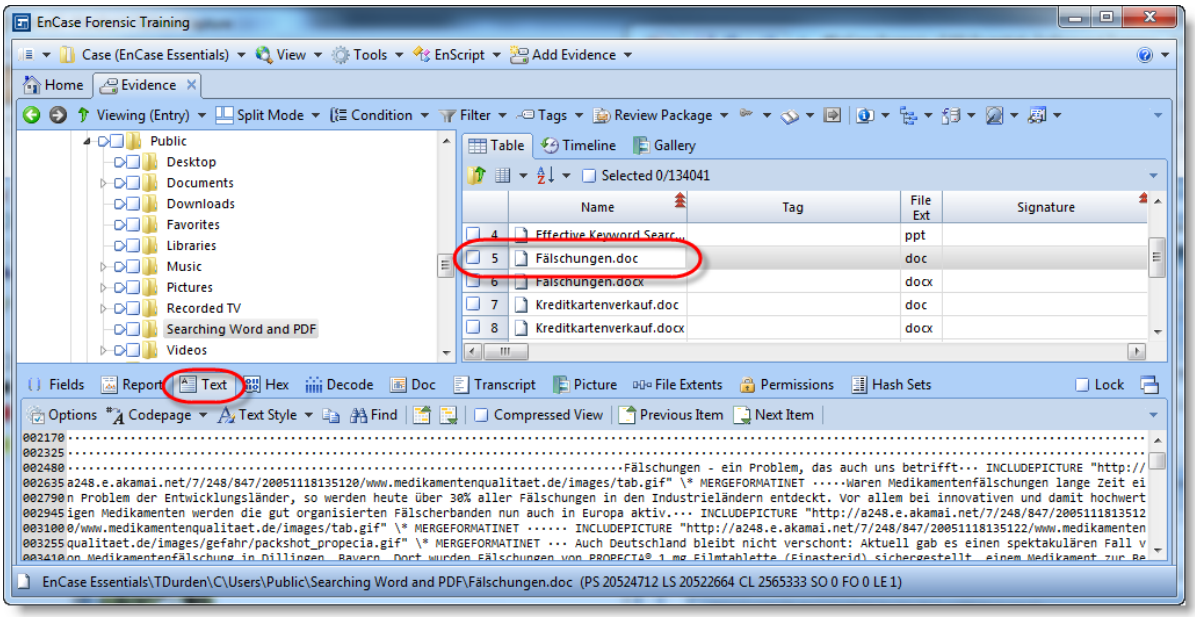

Figure 4-30 Document file in the View Pane – Text tab

Although the text is readable, its format can be improved by altering the text style from the Text Styles menu in the View Pane.

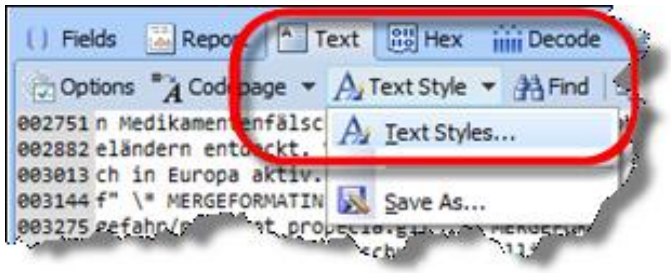

Figure 4-31 Changing text style for View Pane

By default, EnCase v7 includes two Unicode and two ASCII code pages:

- **Unicode** - Fit to page
- **Unicode** - Line breaks at 120 characters
- **ASCII (Western European)** - Fit to page
- **ASCII (Western European)** - Line breaks at 120 characters

Click **New** to create a new text style. Give it a name, such as "German – Line Breaks," and then select the line **Wrap** or **Line Breaks**. The changes will be displayed immediately in the View Pane.

Click on the **Code Page** tab to select the code page.

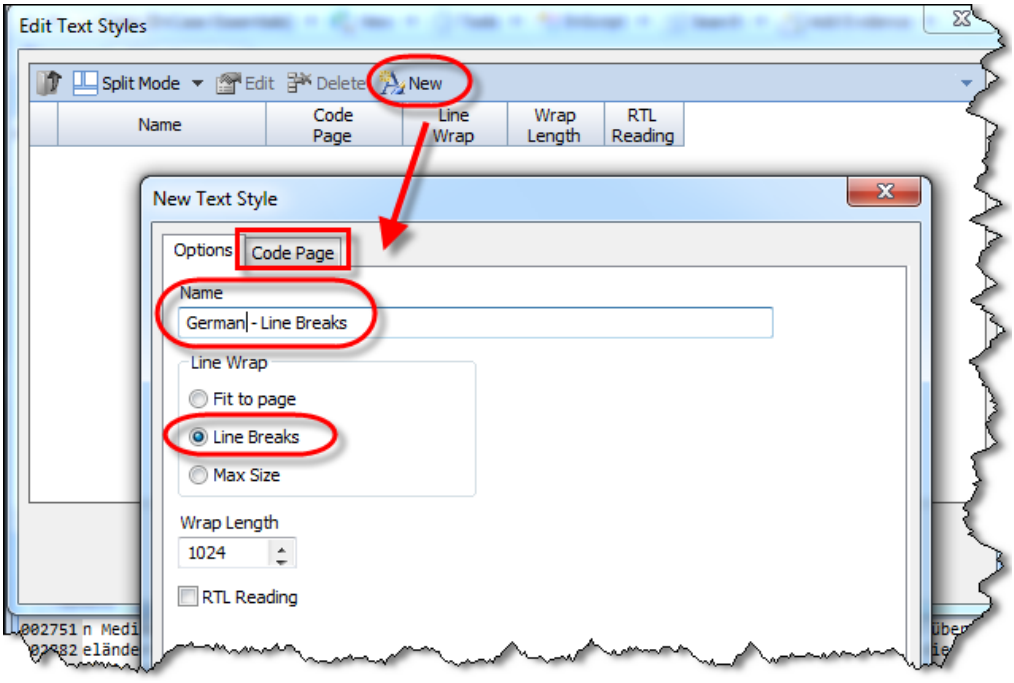

Figure 4-32 Creating a new text style

Click **OK** to save the new text style.

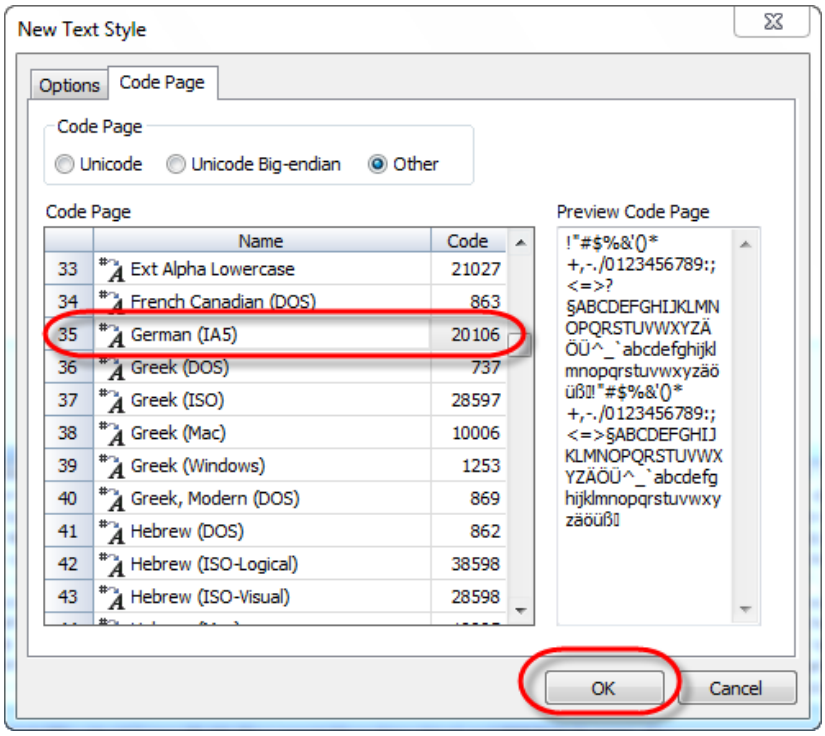

Figure 4-33 Selecting the code page

Click **OK** to have the new code page available.

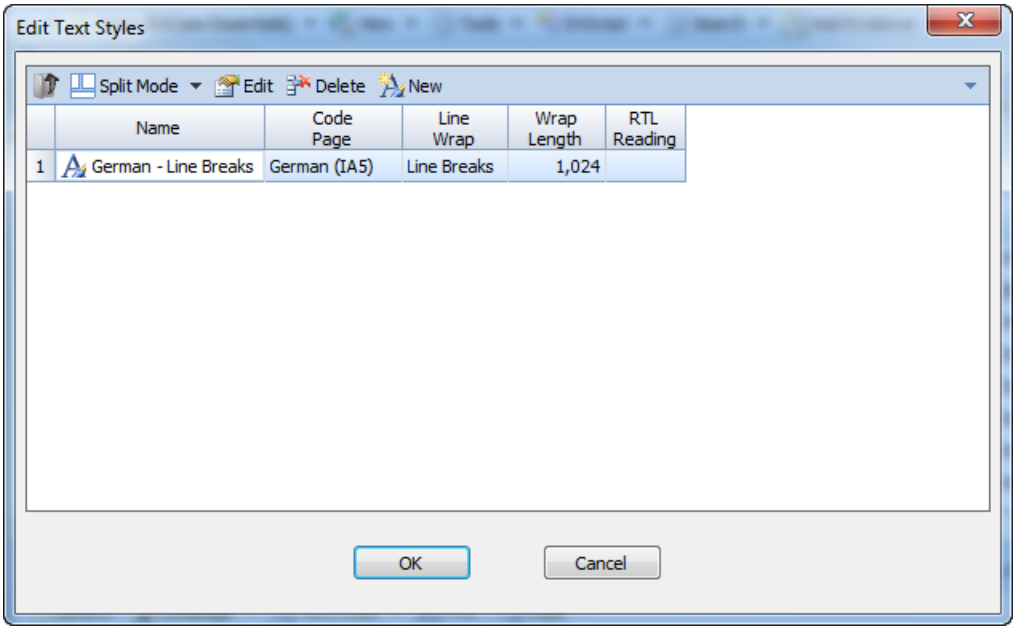

Figure 4-34 New text style

The new text style is now applied to the Text tab in the View Pane

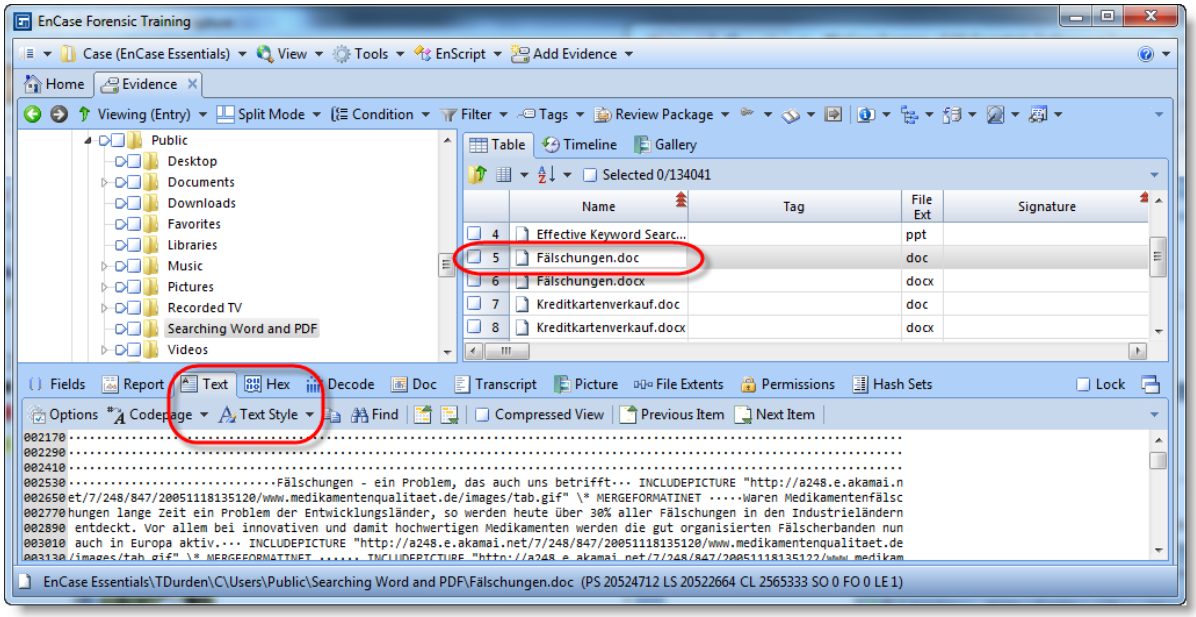

Figure 4-35 Text tab in View Pane

Doc

Here is the same document file displayed in Doc view where it is converted to appear as in the authoring application, Microsoft® Word.

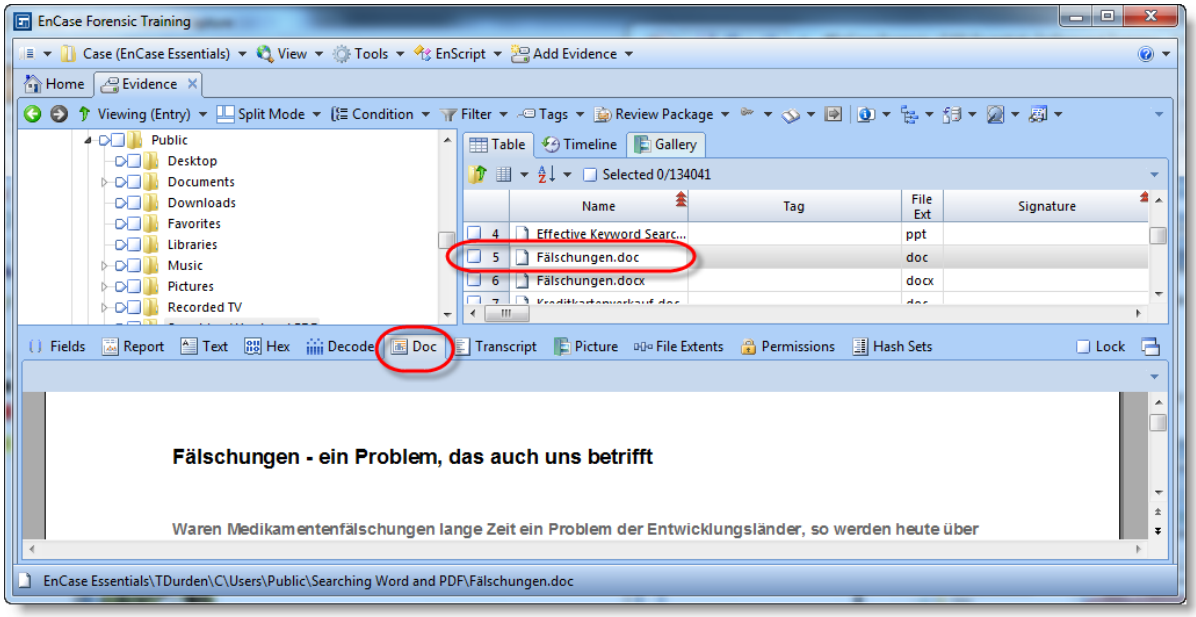

Figure 4-36 DOC file in the View Pane – Doc tab

Transcript

The Transcript tab displays the extracted text from the file. This is the searchable text when conducting a Transcript search with the Index, such as Microsoft® 2007 and 2010 files, including .docx, xlsx, and pptx.

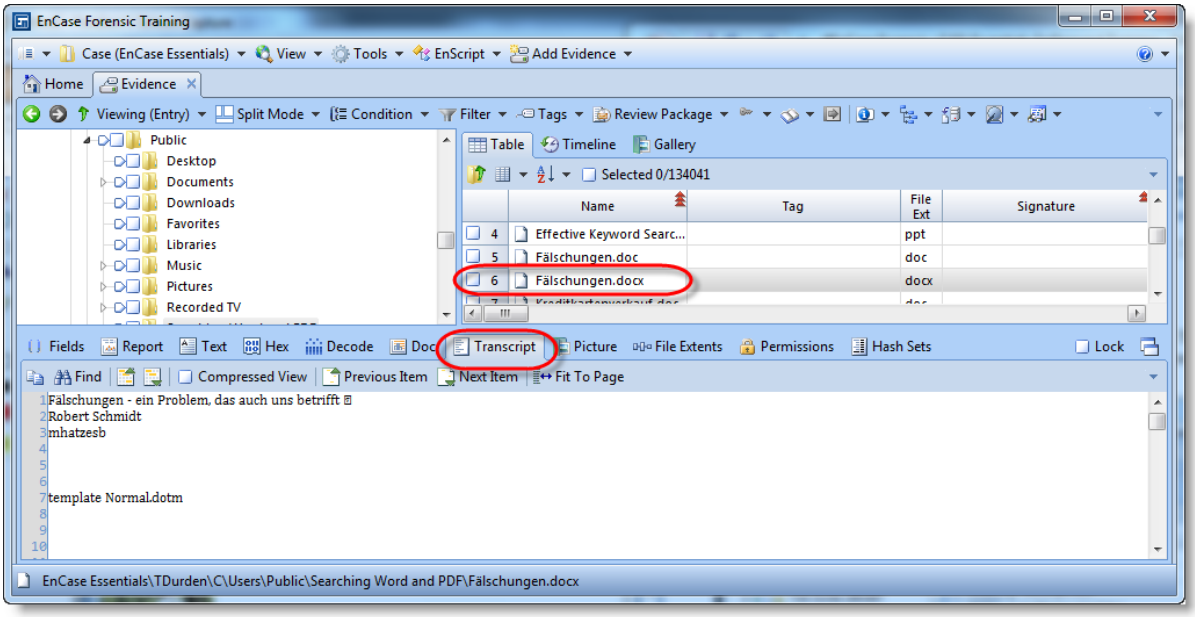

Figure 4-37 DOCX file in the View Pane – Transcript tab

Permissions

The Permissions tab displays the security permissions for a file, including the name and security identification number (SID) of the user(s) who have permission to read, write, and execute a file.

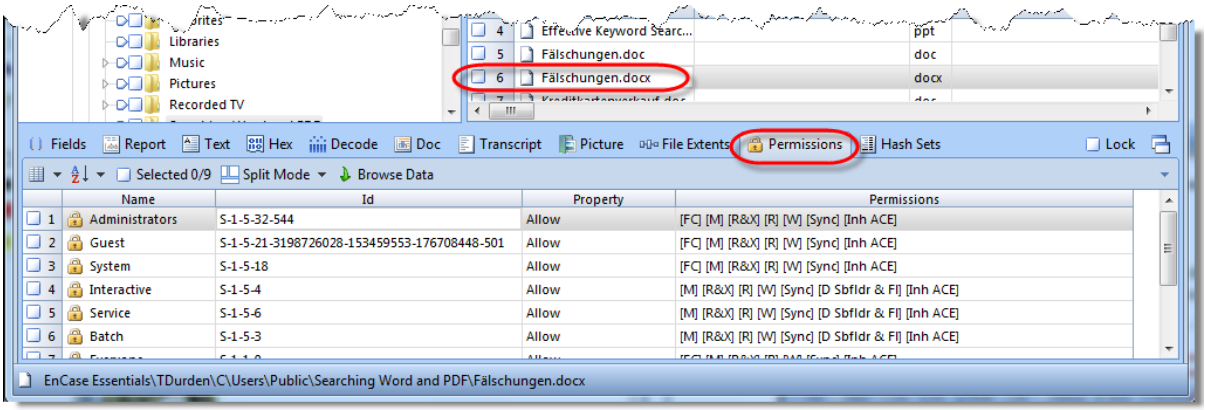

Figure 4-38 DOCX file in the View Pane – Permissions tab

Picture

EnCase checks the contents of the file highlighted in the Table Pane to see if it is an image that can be decoded internally. If so, EnCase will provide the ability for you to select the Picture view in the View Pane and display the image.

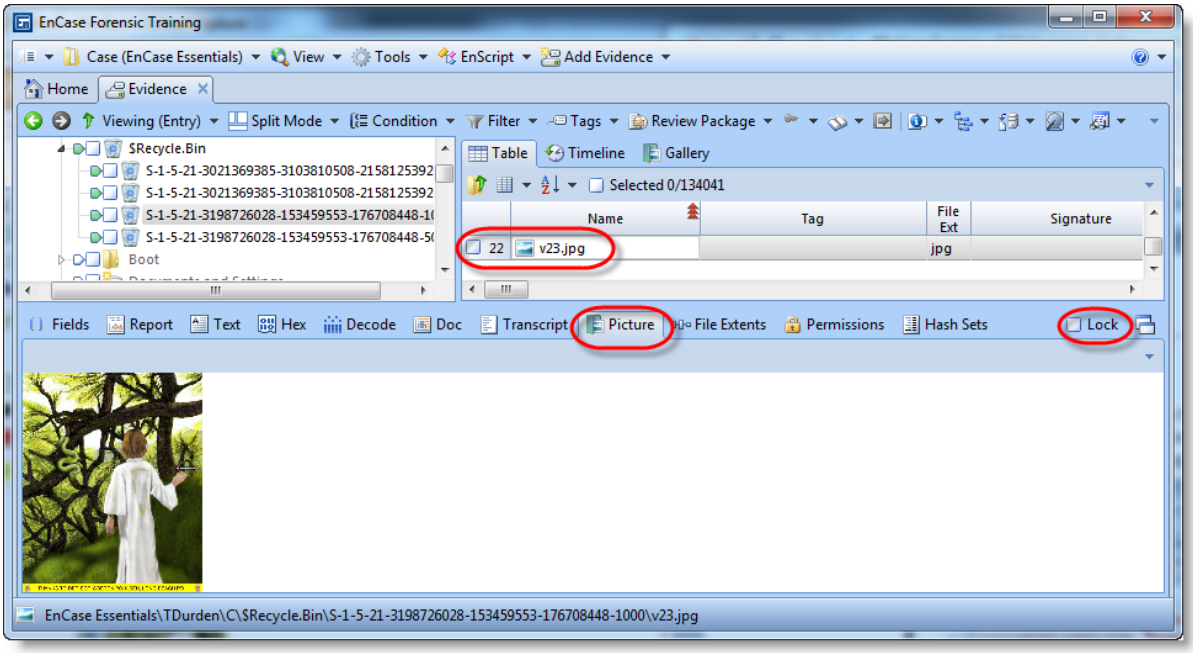

Figure 4-39 Picture view in View Pane

If numerous files highlighted in the Table Pane are images, EnCase v7 will default to the Picture view for subsequent images. If a Microsoft Word document is then highlighted, EnCase v7 will change the default view in the View Pane to Text.

If you wish to have every highlighted item displayed in Hex or Text view, you need only click on the square beside **Lock** to lock that view. To unlock the view, remove the blue-check from the box.

Hex

The following screenshot displays the same picture viewed in hexadecimal.

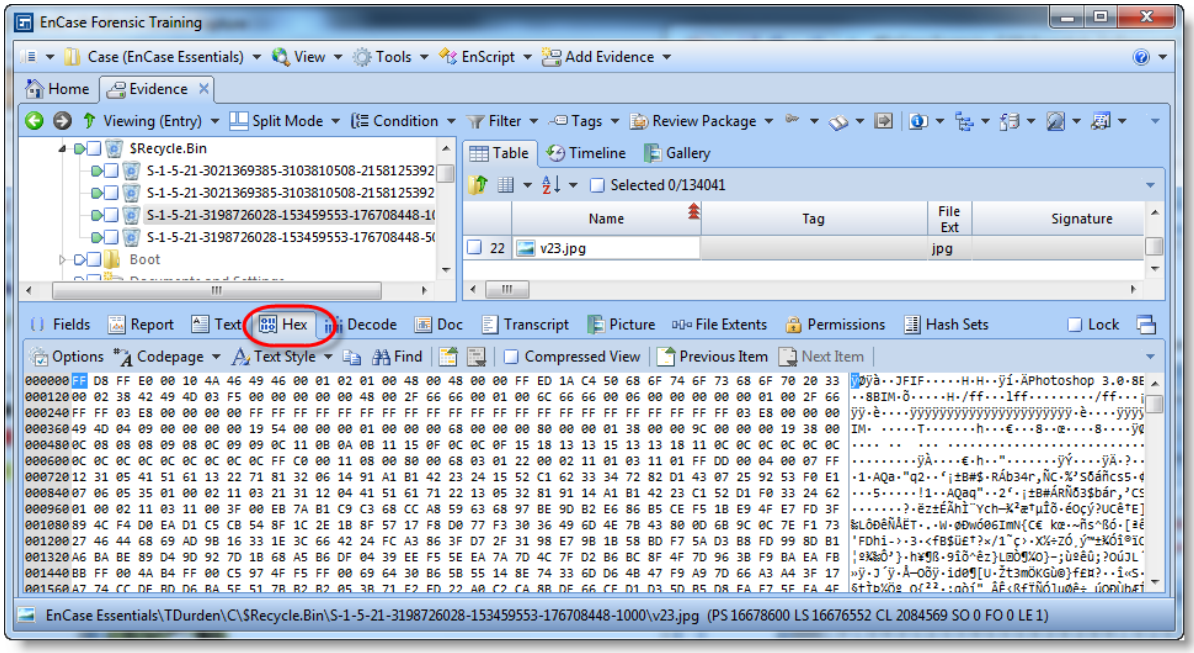

Figure 4-40 Viewing a picture in the View Pane as Hex

Status Bar

It is important to be aware of your current positioning within the case, especially when documenting the location of evidence found in unallocated space. The status bar found at the bottom of the screen will provide that information.

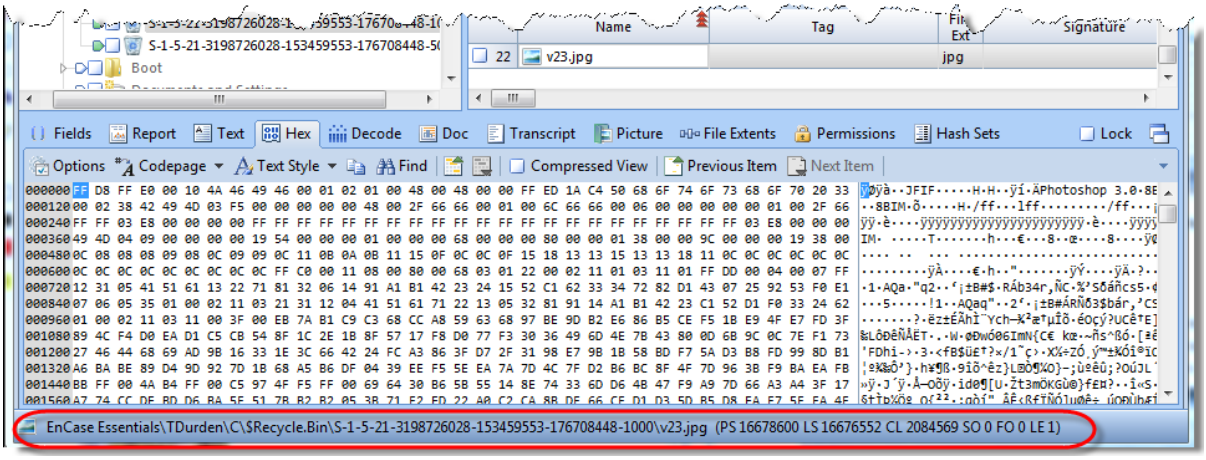

Figure 4-41 Location of status bar

The abbreviations represent:

- **PS** Physical sector number
- **LS** Logical sector number
- **CL** Cluster number
- **SO** Sector offset – The distance in bytes from the beginning of the sector
- **FO** File offset – The distance in bytes from the beginning of the file
- **LE** Length – The number in bytes of the selected area

The status bar also shows the full path of the item highlighted. If a deleted/overwritten file is highlighted, it indicates the overwriting file.

Full-path information is available on all tabs that have the Item Path column (Entries, Records, Search Results, and Bookmarks, as examples). The sector information is available on the Entries and Disk views.

Notes

Notes

Notes

Processing Evidence Files

Evidence Processor

After adding evidence to a case and confirming that the data is valid and browsable, the first task you undertake is to run the EnCase® Evidence Processor. The Evidence Processor lets you run, in a single automated session, a collection of powerful analytic tools against your case data. Since you can run the Evidence Processor unattended, you can work on other aspects of the case while this tool is processing data. After completion, the case data will be processed and ready for you to begin the important analytic and reporting phases of your investigation.

Evidence Processor functions fall into two categories:

- Preparation
- Processing

Before using the Evidence Processor:

- There must be evidence in your case to process
- If you are previewing a device, you must acquire that device prior to processing or as part of the processing
- You should confirm that time zone settings for the evidence are configured properly

  NOTE: EnCase® v7 will utilize the time zone setting of your examiner workstation if no time zone is set for the evidence.

DETERMINE THE TIME ZONE SETTING

Before running the core tasks of the EnCase Evidence Processor, you should confirm the time zone setting of the device.

This information is found in the SYSTEM registry hive for Windows 2000, XP, Vista, and 7. The SYSTEM hive is located in `C:\Windows\System32\Config`.

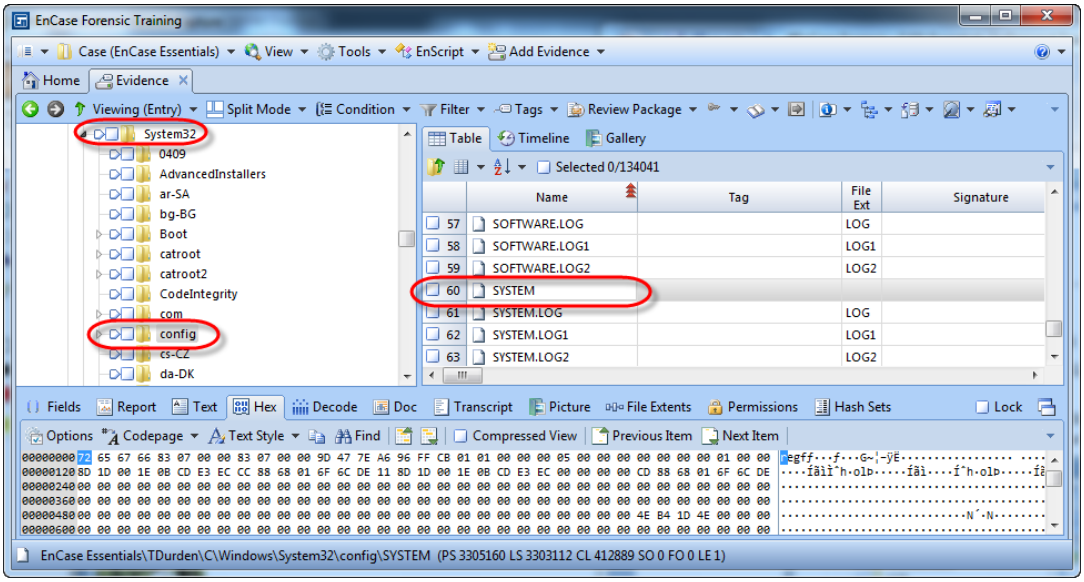

Figure 5-1 SYSTEM hive

To view the data in the SYSTEM hive, use the View File Structure feature in EnCase v7. With the SYSTEM hive selected in the Table Pane, right-click on the file or use the Entries drop-down menu. Select **Entries→View File Structure**.

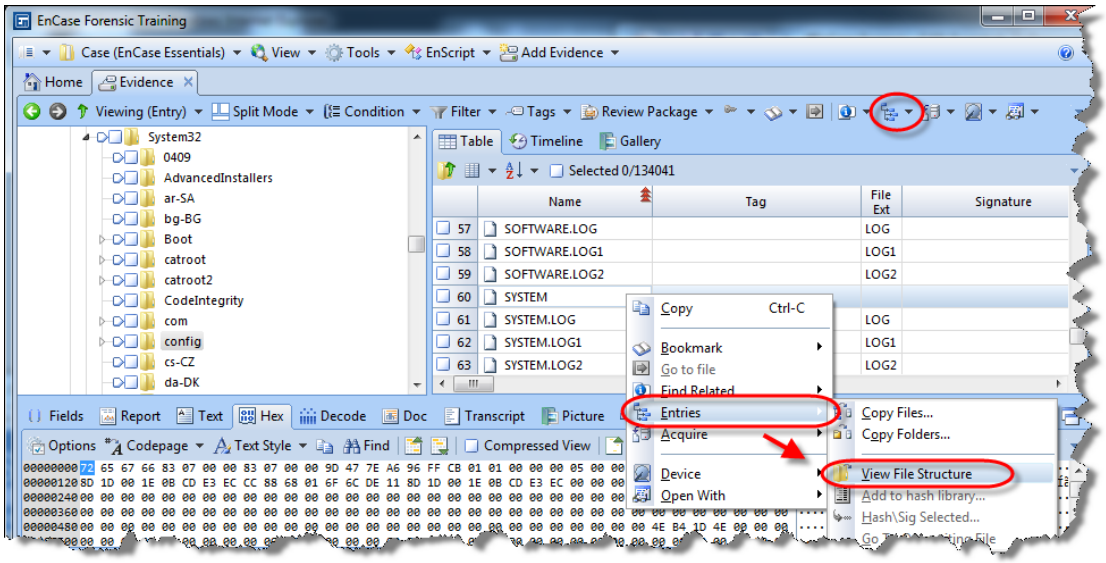

Figure 5-2 View File Structure

EnCase v7 will read the header of the file to detect if it can be processed. You have the option to calculate the unallocated space of the compound file and find deleted content. Click **OK** to begin the parsing process.

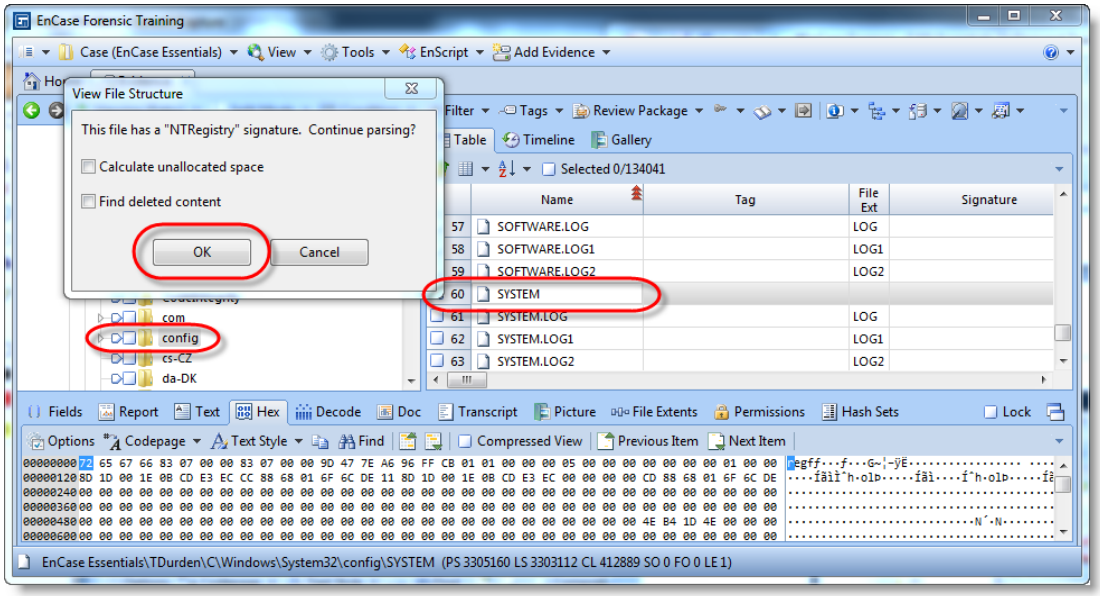

Figure 5-3 View File Structure – Continue parsing

EnCase v7 will scan and parse the registry file and then build a cache file. This allows the file structure of the registry to be written to disk rather than stored in RAM as in previous versions of EnCase.

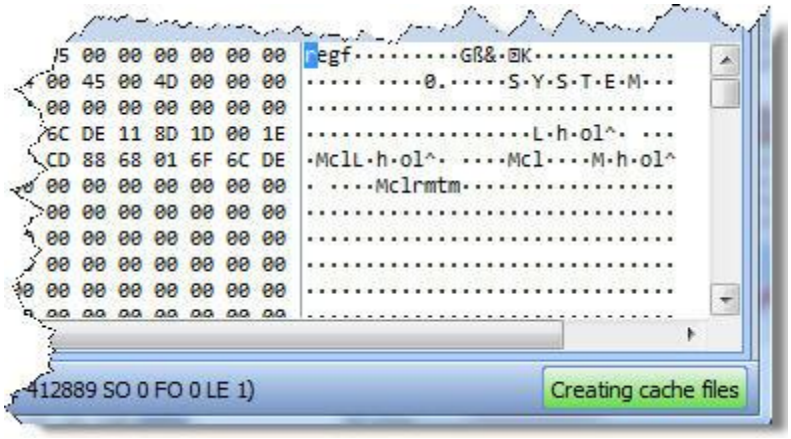

Figure 5-4 Creating cache file for the registry hive

When the parsing is completed, a plus icon (**+**) will appear and the file name will become a hyperlink, indicating it is a processed compound file. Double-click on the file to open the file cache for examination.

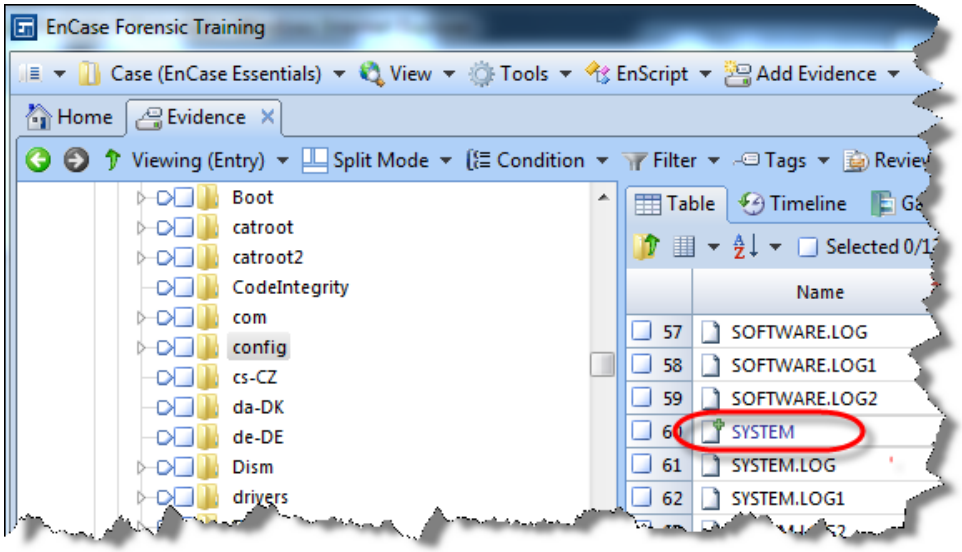

Figure 5-5 Double-click on hyperlinked file name

The time zone setting is stored at:

```
HKEY_LOCAL_MACHINE\System\ControlSet001\Control\TimeZoneInformation\
TimeZoneKeyName
```

Browse the registry file to that location to find the text string with time zone. On the TDurden evidence, it is set to Pacific Standard Time.

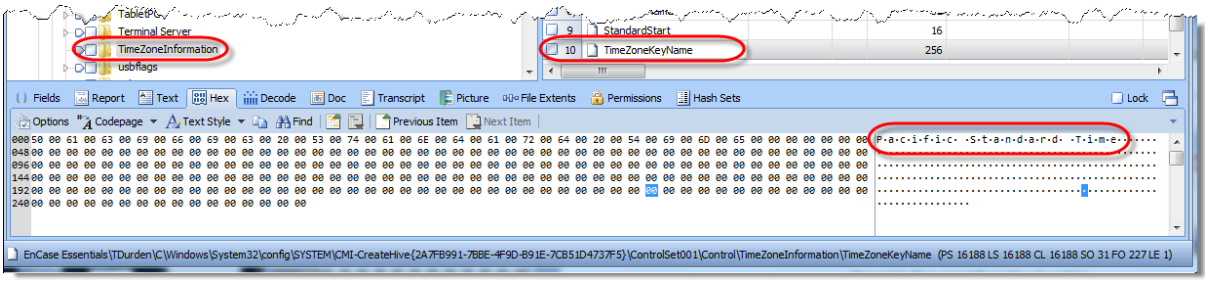

Figure 5-6 Time zone information in registry

Check to confirm the dynamic Daylight Time disabled is **off** (indicated by Hex 00 00 00 00). This means daylight saving time is indeed utilized for this device.

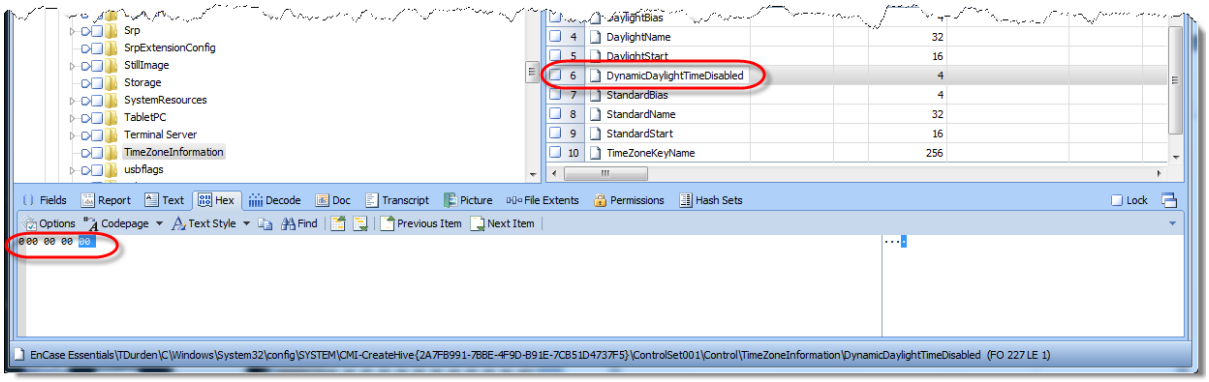

Figure 5-7 Daylight Savings

Use the back button to return to the main Evidence tab.

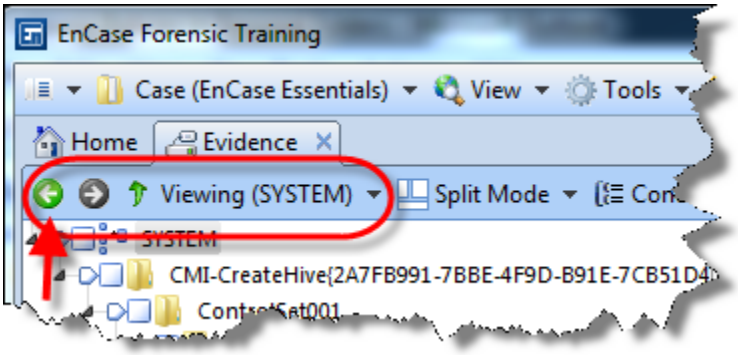

Figure 5-8 Back to Evidence tab

CONFIGURING TIME ZONE SETTINGS

To configure time zone settings:

1. Go to the main **Evidence** tab
   - A list of your devices displays in the Table Pane

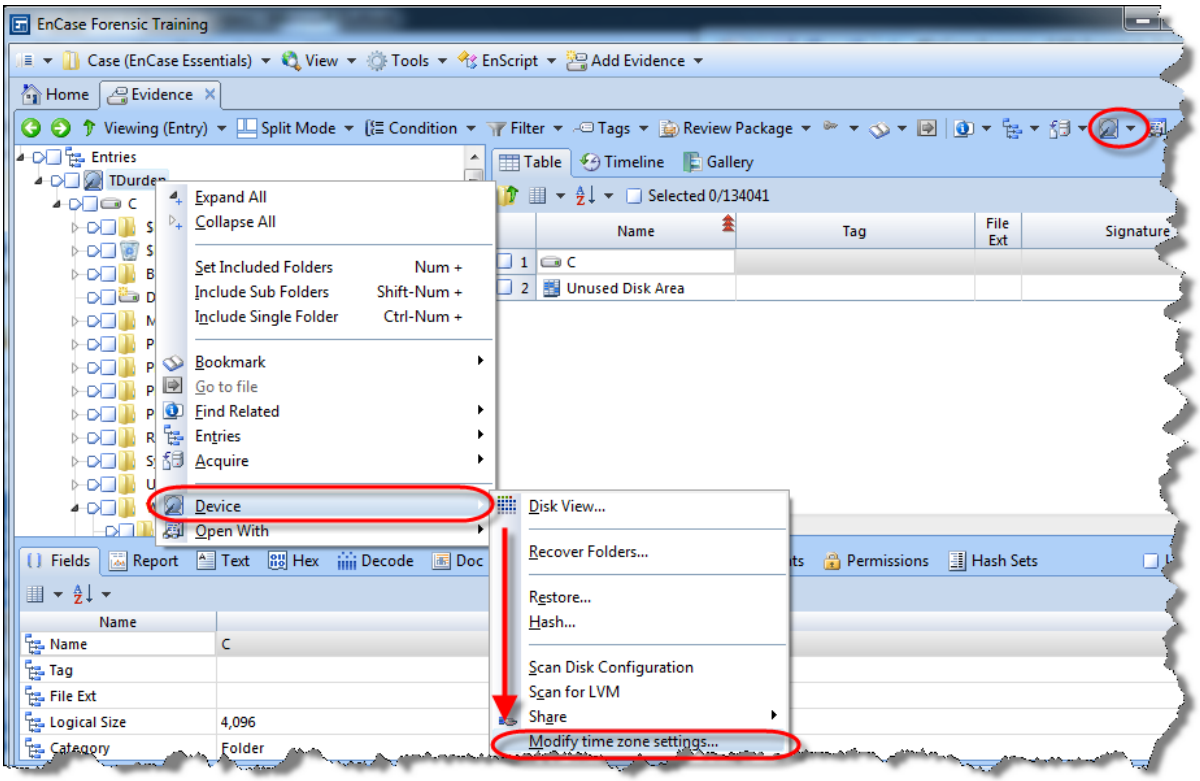

Figure 5-9 Back to the main Evidence tab

2. Right-click on the **TDurden** evidence file
3. Right-click on **Device** in the context drop-down menu
4. Click **Modify time zone settings...**
   - The Case Time Settings dialog appears

5. To aaccount for daylight savings time, select the **Pacific Time (US & Canada)** time zone, and click **OK**

NOTE: The daylight saving time start-and-end dates changed in 2007. You have the ability to choose which version to apply.

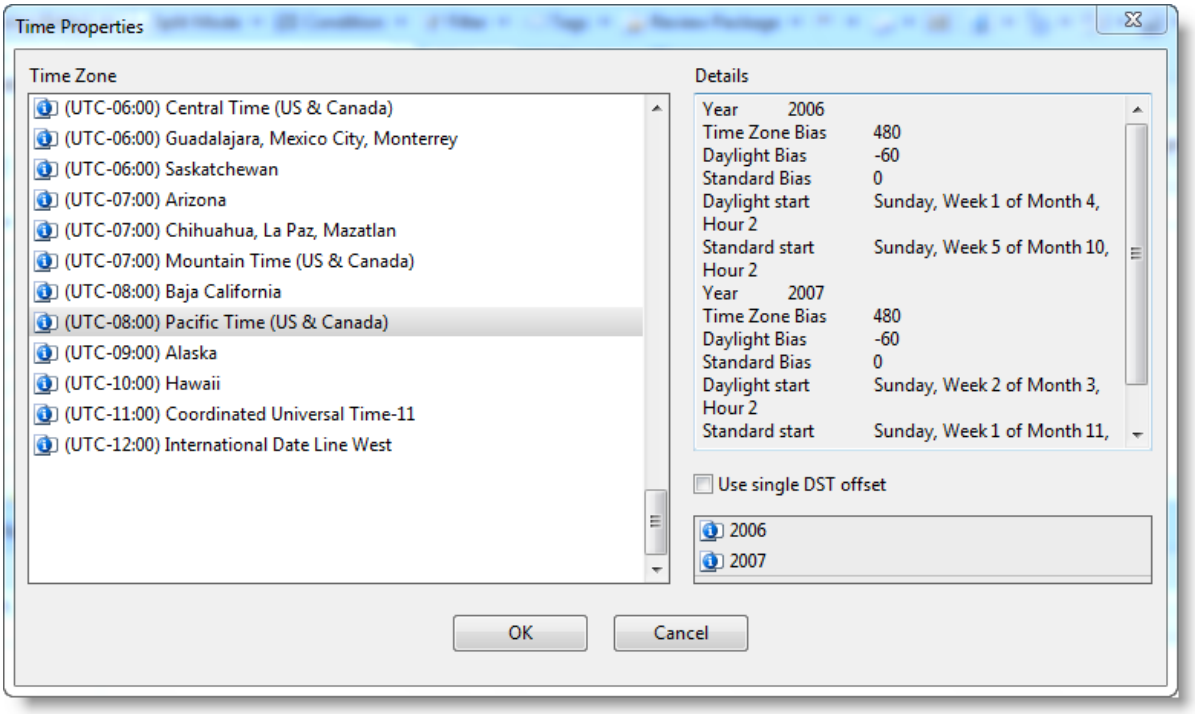

Figure 5-10 Changing the time zone setting

Preparing the Evidence to Process

Now that you have the evidence added and the time zone set, you can process the evidence.

As a reminder, oonce you have added evidence to your case, you must:

- Acquire the evidence (if not already acquired).
- Select the evidence that you intend to run through the Evidence Processor.
- You can add options in the Evidence Processor as you continue an investigation. For example, you may want to run certain options in the beginning, such as file signature and hash analysis, then later add other options, such as parsing compound files. You can select additional options on subsequent Evidence Processor runs, however, you cannot remove previously run options.
- You need to run certain options at a particular time. For example, you must run Recover Folders in the initial processing step. Options you must run in a specific step are marked with a flag icon. An option with a lock icon indicates settings for that option cannot be changed.
- You can run modules over and over again with different settings each time. The results of each run are added to the case.
- You cannot process previously processed and unprocessed evidence together. Also, previously processed evidence must be processed with the same options in order for it to be processed together. All evidence processed at one time must use the same settings.

To acquire and/or run select evidence through the Evidence Processor in a single operation, select **Process Evidence…** from the Add Evidence menu.

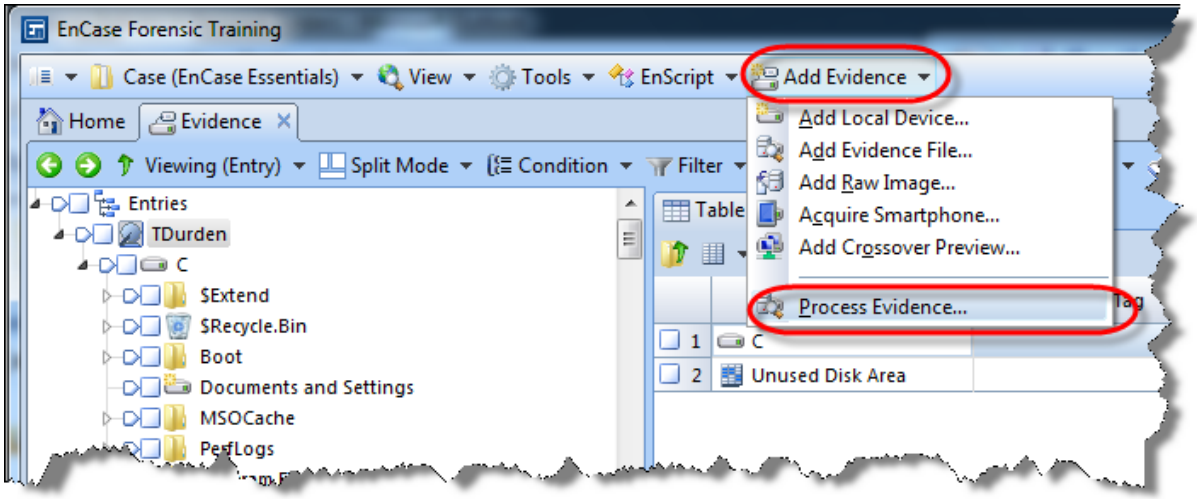

Figure 5-11 Process Evidence…

It will take a few moments to initialize the Evidence Processor and you will see the status in the bottom right corner.

You can run the Evidence Processor using a template with saved or preconfigured settings or you can select the analytic tools to enable and customize their settings prior to running it. If additional evidence becomes available at a later date, you can always rerun the same options on that data.

The Evidence Name pane contains checkboxes for acquiring and processing evidence. Note that you must acquire previewed evidence before you can process it. Initially, the checkboxes in the Evidence Name pane are cleared. Check the boxes for the evidence you want to acquire and/or process. If you have already acquired an item of evidence named in the list, you do not need to check the Acquire box for that item.

In the following example, we acquire devices "1" and "RAM" by checking their boxes under **Acquire** and set them up for processing by checking their boxes under **Process**.

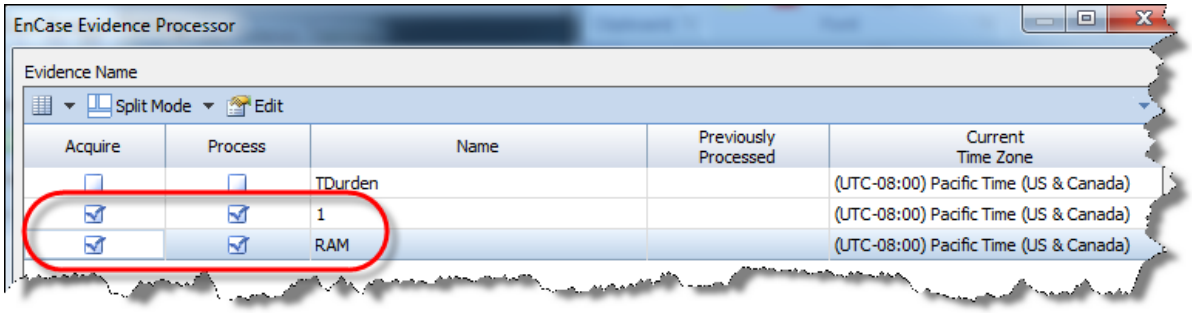

Figure 5-12 Example of acquiring and processing evidence

Managing Evidence Processor Settings

The lower left pane of the Evidence Processor dialog contains a table with the following elements:

- A toolbar
- A list of the Evidence Processor tasks
- A checkbox that allows you to enable (or disable) each task

Use this pane to choose the processor settings to run and to configure their settings.

Using the Processor Settings Toolbar

File and edit settings for the Evidence Processor selections pane are located in its toolbar.

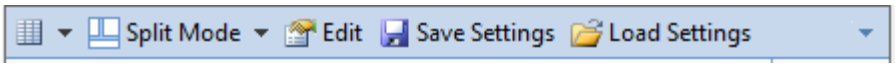

Figure 5-13 Evidence Processor toolbar

Setting	Description
Split Mode	Change the display format of the options pane
Save Settings	Save the current selection of settings as an Evidence Processor template
Load Settings	Load a saved template to run against the current data
Edit	Edit the options for a selected task in the window
Drop-down side menu	Allows you to perform actions, such as printing the results and changing the layout of the Evidence Processor panels